Cuda 12000 IP Access Switch
CudaView Administration Guide

Release 3.0

PART NO.
780-000004-02.A1
PUBLISHED OCTOBER 2001

http://www.adc.com

**ADC Telecommunications, Inc.
8 Technology Drive
Westborough, MA 01581**

ADC Telecommunications, Inc. (herein referred to as "ADC") may revise this manual at any time without notice. All statements, technical information, and recommendations contained herein are believed to be accurate and reliable at the time of publication but are presented without any warranty of any kind, express or implied, (including the warranties of merchantability and fitness and against infringement or interferrence with your enjoyment of the information) and you are solely responsible for your use of this manual with any equipment or software described herein.

The CUDA 12000 is listed to UL 1950 Third Edition and CAN/CSA-C22.2 No. 950-95 Third Edition compliance.

The following information is for compliance by Class A devices with FCC regulations: the equipment described in this manual has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC regulations. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case you will be required to correct the interference at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following methods.

- Turn television or radio antenna until the interference stops.
- Move equipment to one side or the other of the television or radio.
- Move equipment farther away from the television or radio.
- Plug equipment into an outlet that is on a different circuit from the television or radio. *(That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)*

Modifications to this equipment that are not authorized by ADC could void the FCC certification and UL approval and negate your authority to operate the equipment.

This manual is provided by ADC on an "AS IS, WITH ALL FAULTS" basis, without any representation or warranty of any kind, either express or implied, including without limitation any representations or endorsements regarding use of, the results of, or performance of the equipment or software, its appropriateness, accuracy, reliability, or correctness. **You assume the entire risk as to the use of this manual. ADC does not assume liability for the use of this manual beyond its original purchase price. In no event will ADC be liable for additional direct or indirect damages including any lost profits, lost savings, lost revenue or other incidental or consequential damages arising from any defects, or the use or inability to use this manual or the equipment or software described herein, even if ADC has been advised of the possibility of such damages.**

The Cuda 12000 includes RSA BSAFE cryptographic or security protocol software from RSA security. The Cuda 12000 contains an integrated DOCSIS-compliant provisioning server. Use of this provisioning functionality is restricted to licensed authorization. ADC will not support provisioning for for your use thereof if you are not authorized by the appropriate software license to use such provisioning.

The equipment and software described herein may be covered by an ADC warranty statement. You may obtain a copy of the applicable warranty by referring to www.adc.com/cable/support and selecting the *technical assistance* link. What follows is a summary of the warranty statement. The summary is not binding on ADC and is provided to you merely as a convenience.

The equipment warranty usually lasts twelve (12) months from point of shipment and the software warranty usually lasts sixty (60) days from the point of shipment. The software warranty covers both functionality as well as the media on which the software is delivered. Neither warranty entitles the customer to receive free and unlimited access for technical assistance. A separate technical support agreement must be purchased for unlimited access to technical support resources.

The equipment warranty only applies to the cost of a replacement component. It does not include the labor charge for installation of the replacement component. During the warranty period, warranty claims will be processed on a 10-day return to factory basis. Once the defective component is returned to the factory, ADC's sole liability under the equipment warranty shall be either:

- To repair or to replace, at ADC's option, the defective equipment component with a new or refurbished component; or
- If after repeated efforts ADC is unable to resolve the defect by repair or replacement, to refund the purchase price of the equipment or component upon return of the defective item.

A working component will be returned to the customer within 10 days after it is received by ADC.

The warranty period for repaired or replaced equipment components shall be the remainder of the original warranty period for the repaired or replaced item or ninety (90) days, whichever is greater.

Equipment warranty claims can be processed on-line through a web interface or directly by a customer support representative of ADC. As part of the standard process for issuing a Return Materials Authorization (RMA), the Customer Support organization will verify all reported failures prior to authorizing a shipment of a replacement part.

The equipment warranty does not cover any of the following events:

- The equipment has been subject to abnormal use, abnormal conditions, improper storage, exposure to moisture or dampness, unauthorized modifications, unauthorized connections, unauthorized repair, misuse, neglect, abuse, accident, alteration, improper installation, or other events which are not the fault of ADC, including damage caused by shipping;
- ADC or an authorized ADC distributor or reseller was not notified by the customer of the equipment defect during the applicable warranty period.

If the software media is unusable such that the software cannot be loaded onto the equipment, ADC will replace the media within 1 business day after ADC is notified through Technical Assistance Center.

During the software warranty period, ADC will provide software updates and/or maintenance releases at no additional charge to resolve any issues where the software does not function according to software specification. In order to receive on-going software maintenance releases after the 60-day warranty period, the customer must purchase the base level technical assistance agreement.

The software warranty does not cover any of the following events:

- Unauthorized modifications to the software or firmware;
- Unauthorized installation of non-ADC software on the Cuda 12000 platform;
- ADC or an authorized ADC distributor or reseller was not notified by the customer of the software defect during the applicable warranty period.

Non-ADC software may be warranted by its developer, owner or other authorized entity as expressly provided in the documentation accompanying such software.

Failures caused by non-ADC software are not covered by ADC's warranty and service activities to remedy such failures will be billed to the customer.

Remote technical assistance will be provided free of charge during the 60-day software warranty period. The hours for support during the warranty period are Monday through Friday from 8:00am to 5:00pm EST.

Additional hardware and software services are available by purchasing an extended service agreement. Contact your account representative or call 1-877-227-9783 for further details.

CUDA 12000 CUDAVIEW ADMININSTRATION GUIDE

ABOUT THIS GUIDE

PART I ADMINISTRATION OVERVIEW

1 CUDA 12000 OVERVIEW

2 GETTING STARTED

6 MANAGING MULTIPLE CHASSIS

7 SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

PART III IP ROUTING

12 CONFIGURING IP ROUTING

ABOUT THIS GUIDE

This chapter introduces you to the *Cuda 12000 IP Access Switch CudaView Administration Guide* and contains the following sections:

- Document Objective
- Audience
- Document Organization
- Notations
- Related Documentation
- Contacting Customer Support

Document Objective

This guide provides information that you need to configure and manage the Cuda 12000 IP access switch using the graphical user interface (GUI).

Audience

The guide is for the network administrator who is responsible for configuring and managing the Cuda 12000 within a headend site. It assumes a working knowledge of network operations, although it does not assume prior knowledge of the Cuda 12000.

Document Organization

The Cuda 12000 IP Access Switch CudaView Administration Guide is organized as follows:

- **Part I: Administration Overview**
  - **Chapter 1: Cuda 12000 Overview** — Provides an overview of product functionality and includes information on how the Cuda 12000 integrates into your network.
  - **Chapter 2: Getting Started** — Introduces you to the Java-based desktop from which you launch the GUI applications for Cuda Network Management and FastFlow Broadband Provisioning Manager (FastFlow BPM) for a single or a multi chassis group.
  - **Chapter 3: CudaView Desktop Tools** — Provides information about the Tools menu, manipulating table information and performance graphing.
  - **Chapter 4: Managing User Accounts** — Provides information and procedures on how to create and configure user accounts for control of management access.
- **Part II: Chassis Administration**
  - **Chapter 5: Chassis Management** — Provides an overview of chassis-wide configuration and related tasks.
  - **Chapter 6: Managing Multiple Chassis** — Provides information and procedures on how to manage groups of Cuda 12000 chassis.
  - **Chapter 7: Simple Network Management Protocol (SNMP)** — Provides procedures for configuring the Cuda 12000 for SNMPv1, SMPV2 and SNMPv3 management.
  - **Chapter 8: Managing System Events** — Describes how to manage event transmission and logging on the Cuda 12000.
  - **Chapter 9: Module Administration** — Provides information and procedures for basic module administration. Also includes information on how to view traffic statistics for each port.
  - **Chapter 10: Packet Over SONET Administration** — Provides information and procedure for configuring POS.
  - **Chapter 11: Fault Management** — Describes the fault management features that you can use to discover and troubleshoot cable modem, module, and link problems.

- **Part III: IP Routing**
  - **Chapter 12: Configuring IP Routing** — Provides information and procedures for configuring IP interfaces and routing protocols, including RIP and OSPF. Also includes information on adding static IP routes and configuring DHCP relay agents.
  - **Chapter 13: IP Packet Filtering —** Allows you to restrict and control IP packet flow over specified cable interfaces. This control of IP packet transmission restricts network access from specified users, devices, and applications.
  - **Chapter 14: Network-Layer Bridging —** Allows a single subnet to span across multiple DOCSIS CMTS modules. NLBG allows you to add the same IP address to multiple physical interfaces throughout the system.
  - **Chapter 15: Creating Route Filters** — Provides information and procedures for creating RIP and OSPF policy-based route filters.
  - **Chapter 16: Configuring DHCP Relay** — Provides information and procedures for configuring DHCP Relay on CMTS interfaces.
  - **Chapter 17: IP Multicast** — Allows you to reduces traffic on a network by delivering a single stream of information to multiple users at one time.
- **Part IV: Cable Modem Termination Systems**
  - **Chapter 18: Configuring Cable Modem Termination Systems (CMTS)** — Provides information and procedures for configuring and managing CMTS RF parameters. Provides instruction on the configuration of downstream and upstream channels and advanced CMTS parameters.
  - **Chapter 19: Configuring BPI Plus Certificates** — Describes how to configure DOCSIS 1.1 BPI+ certificates.
  - **Chapter 20: Managing Cable Modems** — Provides information for monitoring and managing cable modem (CM/MTA) activity on the network.
  - **Chapter 21: Configuring Subscriber Management** — Describes how to configure subscriber traffic filtering for cable modems and Customer Premise Equipment (CPE) devices.
  - **Chapter 22: Browsing MIBs** — Provides information on how to browse cable modem and MTA MIBs, and the MIB objects that are returned.

Appendices

Appendix A: **Configuring External Provisioning Servers** — Provides information on configuring external provisioning servers.

Appendix B: **Glossary** — Provides a glossary of networking terms used within the Cuda 12000 IP Access Switch Administration guides.

Index

Notations

Table 1 lists the text notations that are used in the Cuda 12000 guides.

Table 1 Notice Conventions

Icon	Notice Type	Description
ⓘ	Information Note	Important or useful information, such as features or instructions
⚠	Caution	Information that alerts you to potential damage to the system
⚡	Warning	Information that alerts you to potential personal injury

Conventions Used in This Guide

- Text formatted in **boldface** indicates a heading, title, name of a folder, window, tab, box, field or button.
- Text formatted in *italics* indicates information that provides important tips about configuration.
- A tooltip provides a description of a tab in a group of options. In addition, a tooltip displays the acceptable values that may be used to configure a parameter. To view a tooltip point the cursor on the tab or in a field.
- Defaults are automatically displayed.
- You must click **Apply** to set the configuration. Clicking Apply for a configuration setting does not *permanently* save (persist) the configuration to the Cuda 12000.
  - This means that the settings are valid only while the module is currently functioning. The next time the module resets it uses the configuration that existed on the management module before changes were made.

To persist a configuration to the management module follow these steps:

1. Go to the menu bar at the top of the window.
2. Go to **File** to **Save**. The configuration is permanently saved to the management module.

A **Reset** button is available for some configuration settings. Perform a Reset if you want to discard new settings, before they are saved, and revert back to the configuration that existed on the management module, before changes were made.

Related Documentation

Refer to the following publications for related Cuda 12000 documentation:

- ***Cuda 12000 IP Access Switch Installation Guide*** — Provides all the information you need to install the system and bring it online. Includes a test procedure to ensure that the system is operational and can provision modems.
- ***Cuda 12000 IP Access Switch CLI-based Administration Guide*** — A procedural guide containing all the information that you need to configure the system using the Cuda 12000 Command Line Interface (CLI).
- ***Cuda 12000 IP Access Switch CLI Reference Guide*** — Provides a command line reference for commands you can use in the Console Interface Window.
- ***FastFlow Broadband Provisioning Manager GUI-based Administration Guide*** — A procedural guide containing all the information that you need to provision cable modems using the graphical user interface (GUI).

Contacting Customer Support

To help you resolve any issues that you may encounter when installing, maintaining, and operating the Cuda 12000 system, you can reach Customer Support as follows:

- Phone: (877) 227-9783 (option 4)
- Customer Support Web Site — To access Customer Support on the Web, go to `http://www.adc.com/cable/support`, then select the *Technical Assistance Center* link. You can then report the problem online, search the ADC Customer Support database for known problems and solutions, and check *Frequently Asked Questions*.

You should have the following information ready, when contacting ADC for technical assistance:

- List of system hardware and software components, including revision levels and serial numbers.
- Diagnostic error messages.
- Details about recent system configuration changes, if applicable.

I ADMINISTRATION OVERVIEW

1 CUDA 12000 OVERVIEW

This chapter explains the overall features of the Cuda 12000 IP access switch; how your Cuda 12000 fits into your network; and the configuration steps it takes to integrate the Cuda 12000 into your network. This chapter consists of the following sections:

- Introducing the Cuda 12000 IP Access Switch
- Understanding Cuda 12000 Within Your Network

Introducing the Cuda 12000 IP Access Switch

The Cuda 12000 IP Access Switch is a fully-meshed IP access switch that sits between the hybrid fiber coax cables (HFC) and the carrier's IP backbone network. It serves as an integrated Cable Modem Termination System (CMTS) and IP router, and supports DOCSIS and EuroDOCSIS RFI Specification 1.0 and 1.1.

To understand the Cuda 12000 IP Access Switch, you need to understand the following aspects of the switch:

- Hardware
- Software
- Minimum Chassis Configuration

Hardware

This section provides a brief overview of Cuda 12000 IP Access Switch hardware features and modules. For more information on Cuda 12000 IP Access Switch hardware, refer to the ***Cuda 12000 IP Access Switch Installation Guide***.

Features

The Cuda 12000 provides the following hardware features:

Table 1-1 Cuda 12000 Hardware Features

Feature	Description
Total System Redundancy	The entire system is architected for full redundancy to provide a highly fault-tolerant solution that includes: ■ Dual-Power Sources: The system can be connected to two -48 VDC power sources to ensure uninterrupted power availability. ■ MeshFlowTM Fabric: Every application module is connected to every other application module via a high-speed serial mesh. This mesh supports a peak throughput capacity of 204.6 Gbps. (132 x 1.55 Gbps.), delivering IP packet routing with minimal latency and high availability to guarantee Quality of Service (QoS) across your core IP network.

Feature	Description
	■ Dual Management modules: The Cuda 12000 supports up to two Management modules to ensure uninterrupted system management. ■ Redundant Management Buses: The backplane consists of a 100-Mbps management BUS with redundant channels, over which the Management modules and system application modules communicate.
Distributed Processing Power	Application modules consist of a network processor with dedicated Synchronous Burst SRAM. Unlike other systems that use a central system processor, processing power and memory scale with every application module that you install in the chassis.
CableOnce™ Network Connections	The system supports a *CableOnce* design that allows you to cable directly to the appropriate connector fixed to the rear of the chassis, or slot backplate. Cabling directly to these stationary connectors, instead of to the modules themselves, allows module replacement without recabling. You remove a module and then insert a new one while the cables remain attached to the system. This blind-mate design also lets you pre-cable chassis slots to prepare them in advance for module installation at a later time.
Hot-swappable Modules	All system modules can be replaced while the system is running without interruption to other interconnected networks. Both application modules and Management modules are hot-swappable.

Modules

The Cuda 12000 IP Access Switch chassis comprises 14 slots. Twelve of the slots are for application modules and two of the slots are for management modules, which control the operations of the chassis. The following is a list of the modules supported by the Cuda 12000 IP Access Switch:

- Management Module
- DOCSIS Modules
  - 1x4 DOCSIS Module
  - 1x4 DOCSIS SpectraFlow Module
  - 1x6 DOCSIS SpectraFlow Module with Spectrum Management

- EuroDOCSIS Modules
  - 1x4 EuroDOCSIS Module
  - 1x4 EuroDOCSIS SpectraFlow Module
  - 1x4 EuroDOCSIS SpectraFlow Module with Spectrum Management
- Egress Modules (Route Server Modules)
  - Octal 10/100 Ethernet SpectraFlow Module
  - Gigabit Ethernet SpectraFlow Module
  - Packet over SONET (POS) SpectraFlow Module

DOCSIS (Data Over Cable Service Interface Specification) is a CableLabs® standard for interoperability between a CMTS and cable modems. EuroDOCSIS (European Data Over Cable Service Interface Specification) is a CableLabs® and tComLabs® standard.

DOCSIS and EuroDOCSIS modules serve as CMTS interface modules with your HFC network using upstream and downstream ports. Upstream ports support both QPSK and 16 QAM modulation; the downstream port supports 64/256 QAM modulation. Each application module has an independent network processor and Synchronous Burst RAM. As a result, processing power and memory scale with every module that you install in the chassis.

The route server module functions in a dual role as both a forwarding device and a route server. The configured route server module is an egress (non-DOCSIS) module, such as an Octal 10/100 Ethernet SpectraFlow Module, Gigabit Ethernet SpectraFlow Module, or Packet over SONET (POS) SpectraFlow Module.

While maintaining its original role as a forwarding module, the route server maintains a central routing table. This module then distributes the routing table to other application modules upon initialization, and incrementally updates the forwarding tables as new routes are discovered. Distributed forwarding tables on each application module provide an added level of fault tolerance; should the Management module or another application module fail, the existing operational modules forward traffic without interruption.

Software

The Cuda 12000 IP Access Switch system software comprises two software components, as follows:

- Base System Software: The base system software is shipped with your Cuda and contains the operating system. The base software includes the command line interface (CLI) and provides you with the following functions:
  - User Account Management
  - Chassis Configuration
  - Multi-Chassis Support
  - Module Administration
  - Event Management
  - SNMP Management
  - IP Configuration
  - Packet and Route Filter Creation
  - DHCP Relay Configuration
  - CMTS Administration
  - Cable Modem Administration
  - Subscriber Management
- CudaView: CudaView provides the graphical interface and full management functionality to the element management system. CudaView offers topology views, fault views, performance graphs, and many other useful features.

Minimum Chassis Configuration

The minimum configuration of the Cuda 12000 IP Access Switch comprises the following:

- A minimum of one management module, plus the base software package. The module and base software are required to configure the Cuda 12000 IP Access Switch.
- An Octal 10/100 Ethernet, Gigabit Ethernet, or POS module. Each of these modules offers these services:

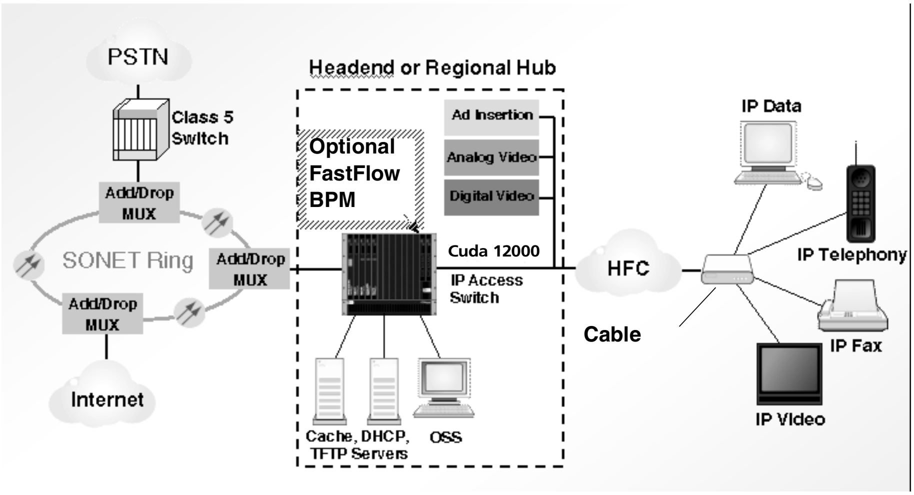
    - A link from the Cuda 12000 to your network backbone
    - May be configured as the route server
    - May function in a dual forwarding role
- One DOCSIS or EuroDOCSIS application module, which is required to perform CMTS functions.
    - May function in a dual forwarding role
- One DOCSIS or EuroDOCSIS application module, required to perform CMTS functionality.

Understanding Cuda 12000 Within Your Network

Cuda 12000 IP Access Switches are installed at the HFC end of a cable plant and are responsible for gateway operations between the headend and the Internet. Through the Cuda 12000 IP Access Switch, digital data signals are modulated onto RF channels for broadcast over the same infrastructure.

Typically, the signals are broadcast through the HFC to fiber nodes in the network. Amplifiers, coaxial cable, and taps carry the signals to the subscriber premises.

This example shows how the Cuda 12000 IP Access Switch can fit into your network.



Cable Modem Termination System (CMTS)

The Cuda 12000 implements DOCSIS and EuroDOCSIS CMTS functionality, providing connectivity and data forwarding for cable modems over the RF cable plant.

The DOCSIS and EuroDOCSIS modules interface with your HFC network, using a 1-to-4 downstream-to-upstream port ratio (referred to as 1 x 4), or a 1-to-6 downstream-to-upstream port ratio (referred to as 1 x 6). Upstream ports support QPSK and 16 QAM modulation; the downstream port supports 64 and 256 QAM modulation.

IP Routing Configuration

The Cuda 12000 IP Access Switch uses the Internet Protocol (IP) to exchange data over computer networks consisting of cable and Ethernet interfaces. In addition, it supports RIP and OSPF routing protocols to exchange routing information with other routers in the IP network.

To integrate the Cuda 12000 IP Access Switch into your network, the following configuration must be accomplished:

- Configure the CMTS interfaces so that the cable modems range properly.
- Provision cable modems, Multimedia Terminal Adapters (MTAs), and CPE (Customer Premise Equipment) devices, using the FastFlow Broadband Provisioning Manager or a third-party provisioning server.
- Configure DHCP subnets, so that the DHCP server gives out IP addresses to cable modems, MTAs, and CPE devices.
- Configure IP on your cable, Ethernet, and Packet Over SONET interfaces to connect the Cuda 12000 to your backbone network and provide the subscribers access to the Internet.
- For the HFC segments, configure DHCP relay to specify the subnet to be used for assigning IP addresses to cable modems, MTAs, and CPE devices.

IP, RIP and OSPF can currently be configured on any of the interfaces within the Cuda12000 IP Access Switch.

2 GETTING STARTED

This chapter introduces you to the CudaView desktop and includes the following topics:

- Before You Begin
- About the Desktop
- Accessing the Desktop
- Navigating the Desktop
- Navigating Folders, Tabs, and Buttons
- Topology View of the Cuda Network

Before You Begin

Before you access the desktop, verify that:

- You have installed the Cuda 12000 as described in the *Cuda 12000 IP Access Switch Installation Guide*.
- You have configured the 10/100 craft management port with a valid IP address appropriate to your network environment, as described in the *Cuda 12000 IP Access Switch Installation Guide*.
- The system is online and accessible. You can verify this by pinging the 10/100 management port on the Management module.
- You have installed the CudaView software component.
- You are using one of the following Web browsers:

  — Microsoft Internet Explorer version 4.0 or greater

  — Netscape Communicator version 4.61 or greater
- You installed the Java 2 Runtime Environment version 1.3 plug-in from Sun Microsystems. The Java Webstart plug-in from Sun Microsystems is optional.

About the Desktop

The desktop provides a Graphical User Interface (GUI) to the Cuda 12000. This Java-based desktop serves as the platform for the management functions that are available, using the Chassis 12000:

- **Cuda Chassis Manager** — Provides access to basic system management, physical interface and chassis configuration, CMTS administration, and other general administration functions.
- **Security Management** — Provides access to all functions relating to managing user profiles.
- **FastFlow BPM 1** — Provides access to cable modem provisioning functions, including DHCP subnet configuration. *For information about FastFlow BPM, refer to Chapter 1, "Cuda 12000 Overview" or the FastFlow BPM administration guides.*

Accessing the Desktop

Ensure that the Cuda 12000 is accessible to the remote system. You access the desktop by using either Microsoft Internet Explorer Version 4.0 or higher, or Netscape Communicator Web browsers on a remote system.

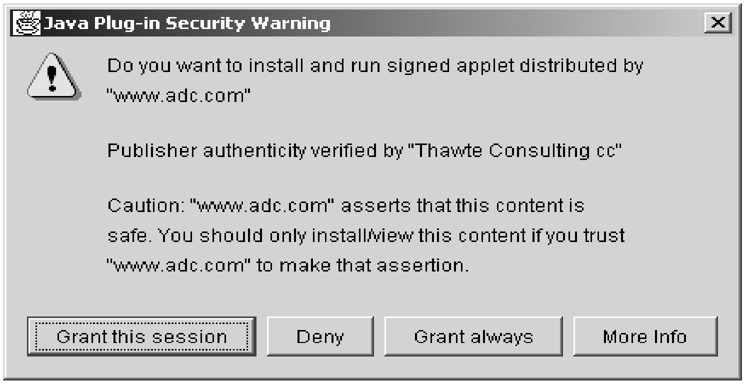
Accessing the desktop involves the following procedures:

- Launching the Web Browser
- Logging into the Cuda 12000

Launching the Web Browser

1. Launch the Web browser — either Microsoft Internet Explorer or Netscape Communicator.
2. In the browser's URL field, enter the IP address of the management port followed by /bas.html; press **ENTER** to access the specified location. For example, xxx.xx.x.xx /bas.html (where "xxx.xx.x.xx" represents the IP address).
3. When the java applet is not installed, the Java Plug-in Security Warning displays (Figure 2-1). Click **Grant this session** to run the java applet for this session only; or, click **Grant always** to install the java applet. When the java applet is installed, the security warning message no longer displays each time you access the desktop.

Figure 2-1 Java Plug-in Security Warning



Java Plug-in Security Warning

Do you want to install and run signed applet distributed by "www.adc.com"

Publisher authenticity verified by "Thawte Consulting cc"

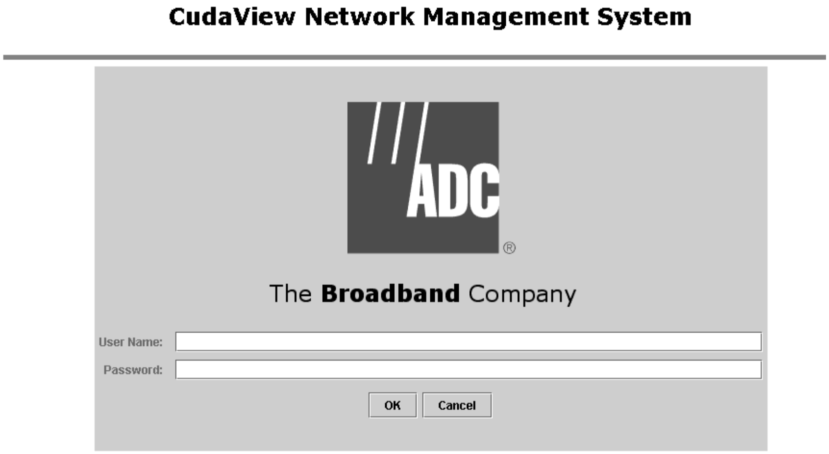
Caution: "www.adc.com" asserts that this content is safe. You should only install/view this content if you trust "www.adc.com" to make that assertion.

Logging into the Cuda 12000

The Cuda 12000 supports two different login windows, which are the following:

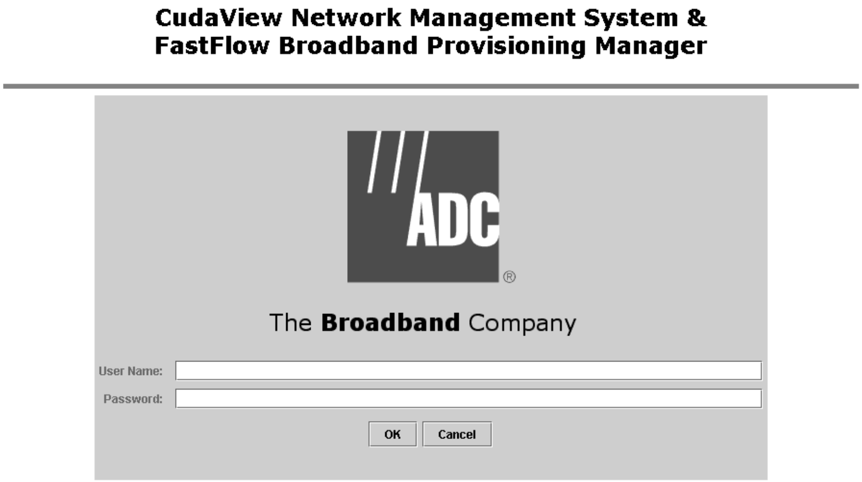
1. **CudaView Network Management** — This login window (Figure 2-2) appears if you install the CudaView software component.

Figure 2-2 CudaView Login Window



2. **CudaView Network Management System & FastFlow Broadband Provisioning Manager** — This login window appears (Figure 2-3) if you install the CudaView and FastFlow Broadband Provisioning Manager (FastFlow BPM) software components.

Figure 2-3 CudaView and FastFlow BPM Login Window



CudaView Network Management System &
FastFlow Broadband Provisioning Manager

To log into either CudaView or CudaView and FastFlow BPM, follow these procedures:

1. Enter your account username and password. The Cuda 12000 ships with the following account information:
   - Username — **root**
   - Password — **bas**
2. Click **OK**. The desktop appears.

As with the login windows, the Cuda 12000 supports two different desktop backgrounds, which are dependent on the installed software components. Figure 2-4 and Figure 2-5, below, display the desktop backgrounds for CudaView, and CudaView and FastFlow BPM. Figure 2-5 adds the **FastFlow BPM 1** folder, which provides the GUI interface for provisioning functions.

Figure 2-4 CudaView Desktop Background]

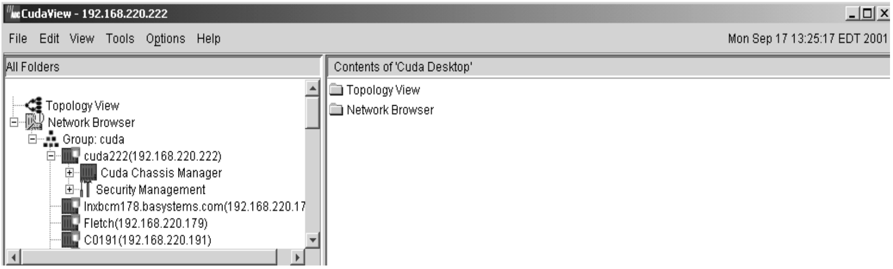
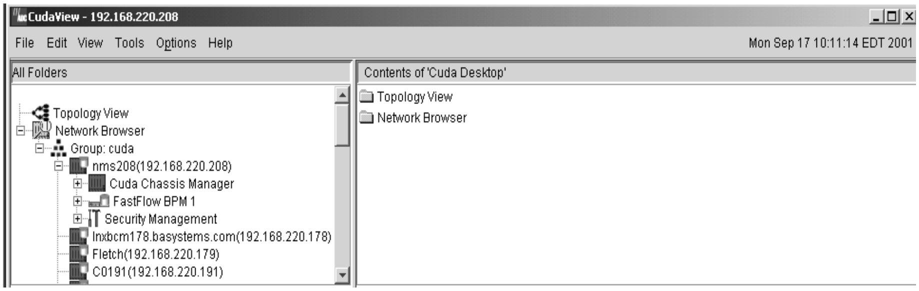


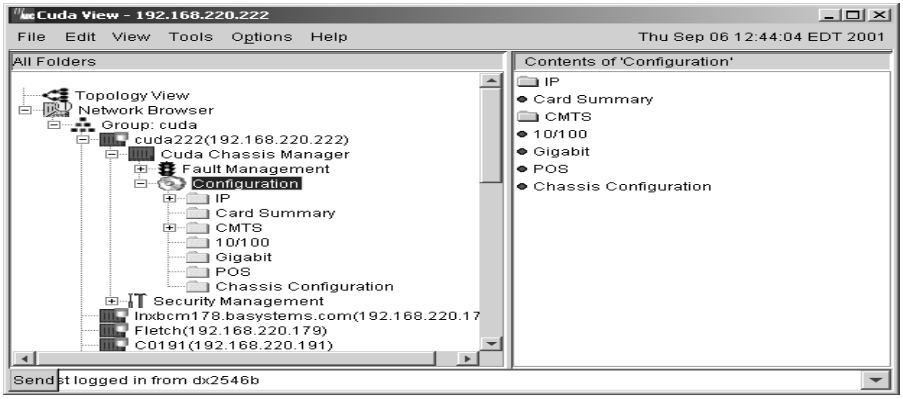
Figure 2-5 CudaView and FastFlow BPM Desktop Background



Navigating the Desktop

The window is divided into two panels. The left panel lists the top-level folders with associated sub-folders in the folder structure. The right panel lists the windows available for configuration. The right panel display results from clicking on the 'Configuration' folder in the left panel. The sub-folders in the right panel comprise a collection of configuration windows. A red diamond identifies a configuration window.

Figure 2-6 Desktop: Both Panels]

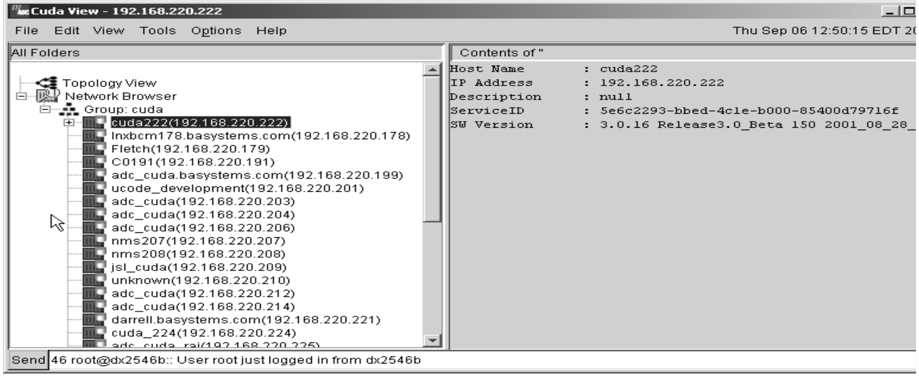


st logged in from dx2546b

To expand or reduce the size of the panels, place the cursor on the divider, left click, and drag the bar to the left or to the right.

Clicking on a chassis-level folder displays network node information in the right panel.

Figure 2-7 Right Panel: Network Node Information


Cuda View - 192.168.220.222
File
Edit
View
Tools
Options
Help
Thu Sep 06 12:50:15 EDT 20
All Folders
Topology View
Network Browser
Group: cuda
cuda222(192.168.220.222)
lnxbcm178.basystems.com(192.168.220.178)
Fletch(192.168.220.179)
C0191(192.168.220.191)
adc_cuda.basystems.com(192.168.220.199)
ucode_development(192.168.220.201)
adc_cuda(192.168.220.203)
adc_cuda(192.168.220.204)
adc_cuda(192.168.220.206)
nms207(192.168.220.207)
nms208(192.168.220.208)
jsl_cuda(192.168.220.209)
unknown(192.168.220.210)
adc_cuda(192.168.220.212)
adc_cuda(192.168.220.214)
darrell.basystems.com(192.168.220.221)
cuda_224(192.168.220.224)
adc_cuda_rai(192.168.220.225)
Contents of "
Send

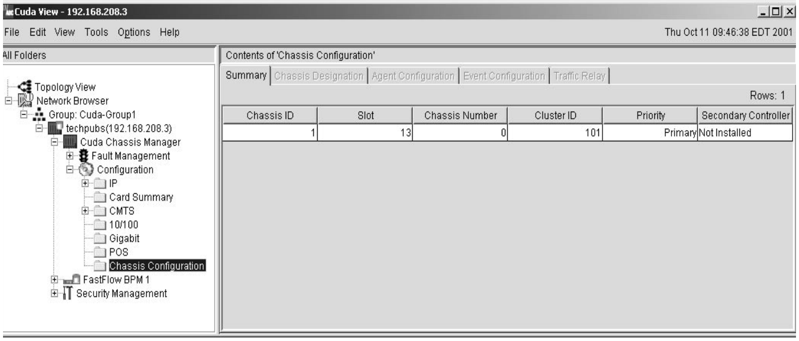
```
Host Name         :  cuda222
IP Address        :  192.168.220.222
Description       :  null
ServiceID         :  5e6c2293-bbed-4cle-b000-85400d79716f
SW Version        :  3.0.16 Release3.0_Beta 150 2001_08_28_
```

46 root@dx2546b:: User root just logged in from dx2546b

Window Layout

The example window (Figure 2-8, “Initial Window Example Opened by Clicking on the Chassis Configuration Folder”) is titled “Contents of ‘Chassis Configuration’," and is opened when you click on the Chassis Configuration folder.

Figure 2-8 Initial Window Example Opened by Clicking on the Chassis Configuration Folder



Thu Oct 11 09:46:38 EDT 2001

Contents of 'Chassis Configuration'

Rows: 1

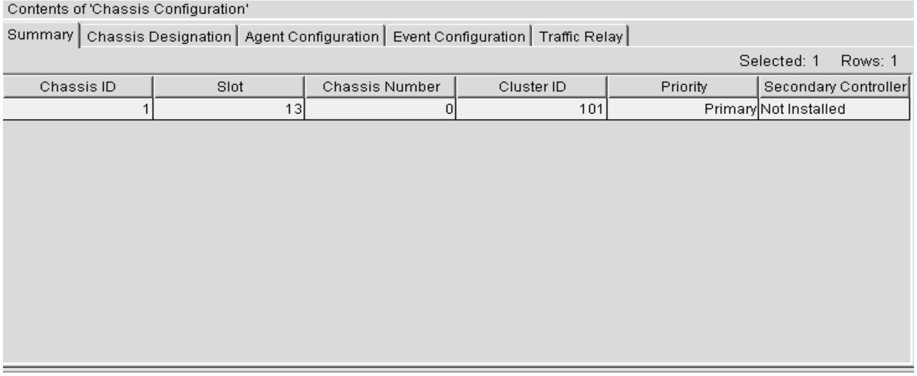
Chassis ID	Slot	Chassis Number	Cluster ID	Priority	Secondary Controller
1	13	0	101	Primary	Not Installed

Window Tabs

The first time that you open a session the left-most tab is displayed and all other tabs within the window are greyed out. A table appears, consisting of column headings and one or more rows, shaded in white. Each row is associated with a module interface.

You select a row by clicking on it. A selected row is shaded in blue and the tabs become active. For example, in Figure 2-9 the row has been selected and the tabs are active.

Figure 2-9 Example: Table Row Selected

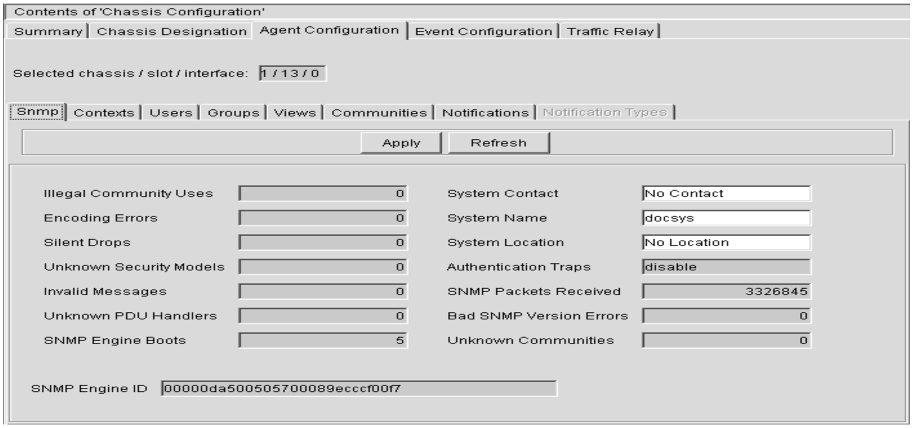


Selected: 1 Rows: 1

Chassis ID	Slot	Chassis Number	Cluster ID	Priority	Secondary Controller
1	13	0	101	Primary	Not Installed

If you click on the **Agent Configuration** tab, you open the window in Figure 2-10“Example: Window Opened by Clicking on the Agent Configuration Tab”. This window also contains a row of tabs. Notice that the tabs are active, since they are associated to the row selected in the Summary window (refer to Figure 2-9.)

Figure 2-10 Example: Window Opened by Clicking on the Agent Configuration Tab



Selected chassis / slot / interface: 1 / 13 / 0

Illegal Community Uses	0	System Contact	No Contact
Encoding Errors	0	System Name	docsys
Silent Drops	0	System Location	No Location
Unknown Security Models	0	Authentication Traps	disable
Invalid Messages	0	SNMP Packets Received	3326845
Unknown PDU Handlers	0	Bad SNMP Version Errors	0
SNMP Engine Boots	5	Unknown Communities	0

SNMP Engine ID 00000da500505700089ecccf00f7

CudaView remembers the last tab of a session, as you navigate through various folders. For example, if you exit Chassis Configuration and start a session within another folder, when you return and open the Chassis Configuration session the Agent Configuration tab is displayed.

Buttons

Buttons occur in windows and dialog boxes to confirm configuration functions. In the above example, the buttons are Apply and Refresh. Throughout this guide, the purpose of the button is explained within the specific configuration procedures.

Parameters

Every window contains either table columns, fields, check boxes, or radio buttons that are associated with parameters.

- Parameters that you can reset have a white background and become shaded blue when selected. You may need to click a field, a table, a check box, or a radio button in order to set values.
- A grey field cannot be set.
  - If the field contains a value, it is read-only;
  - if empty, the field is currently not available for setting or viewing.

Navigating Folders, Tabs, and Buttons

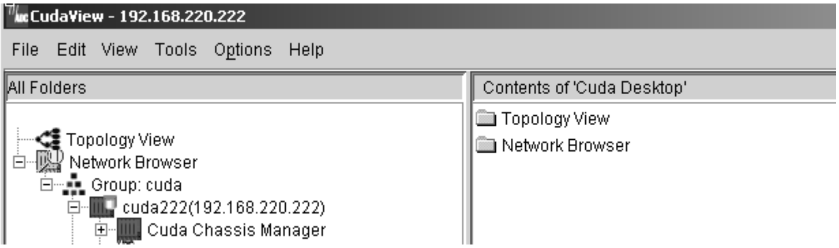
This guide provides you with navigation sequences and any additional steps that are needed to open windows and perform management functions.

Navigating Folders

To open any window, you will always need to navigate through the following sequence of folders as part of the navigation path:

Network Browser > *GroupName*> *ChassisName*> **Cuda Chassis Manager**

Figure 2-11 Partial Path Through Folders



- ***GroupName*** is the name of the group that you may use instead of the default group name 'Cuda' that is shipped with your chassis. In the window above, *GroupName* is 'Cuda'.
- ***ChassisName*** is the name of the chassis that you access within your network. In the example above, *ChassisName* is 'Cuda222'.

The following is an example of a complete folder sequence:

Folders: **NetworkBrowser>Cuda>Cuda222>Cuda Chassis Manager>Chassis Configuration**

The right-most folder in the sequence is the folder that you must click on before a window opens; for example, refer to (Figure 2-8, "Initial Window Example Opened by Clicking on the Chassis Configuration Folder"). In this example, when you click on the Chassis Configuration folder, the Chassis Configuration window opens.

Navigating Tabs

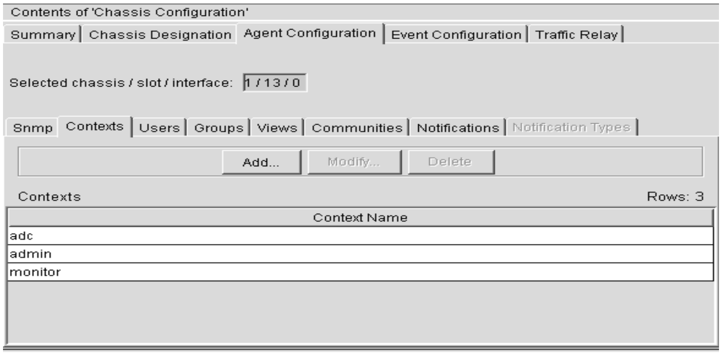
After navigating a sequence of folders, you may need to navigate a sequence of tabs to open a window.

The following is an example of a tab sequence:

Tabs: **Agent Configuration>Contexts**

Each tab in a tab sequence brings up a separate window. The right-most tab in this sequence is the tab that you need to click to open the window being described.

Figure 2-12 Example of a Window After Tab Sequence



Selected chassis / slot / interface: 1 / 13 / 0

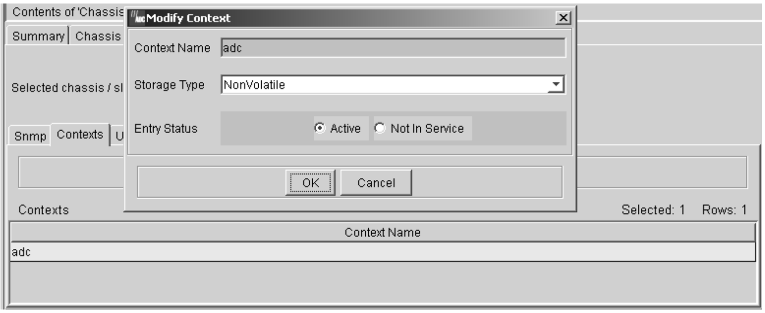
Contexts Rows: 3

Context Name
adc
admin
monitor

Using Buttons

After navigating a sequence of folders or tabs, you may need to click a button to complete a function or even to bring up another window. Before you click a button, you may need to select the object. In Figure 2-12, the Context Name "adc" is selected to be modified. Clicking the Modify button in Figure 2-12 results in the following window example (Figure 2-13. “Window After Clicking Modify Button”).

Figure 2-13 Window After Clicking Modify Button



Context Name: adc

Storage Type: NonVolatile

Entry Status: ● Active ○ Not In Service

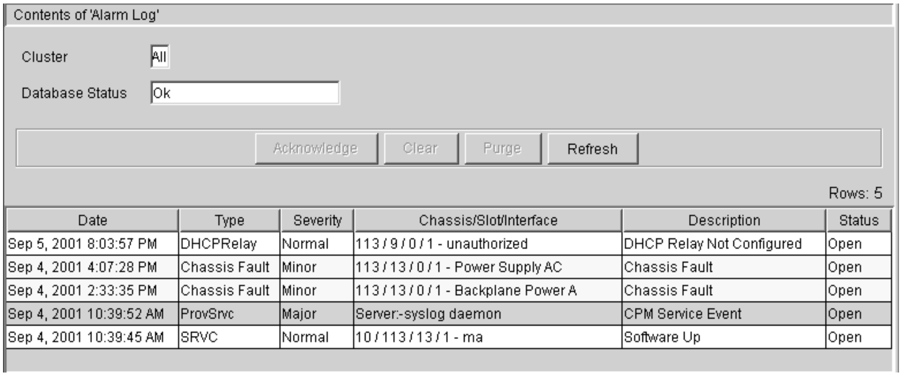
Context Name
adc

Greyed Out Buttons and Tabs

A button or a tab is greyed out for either of two reasons:

- The button or tab is active only for certain network configurations.
- You need to select a row, a field, a radio button, or click in a particular box, to active the button or tab.

Figure 2-14 Example: Greyed Out Buttons



Cluster: All

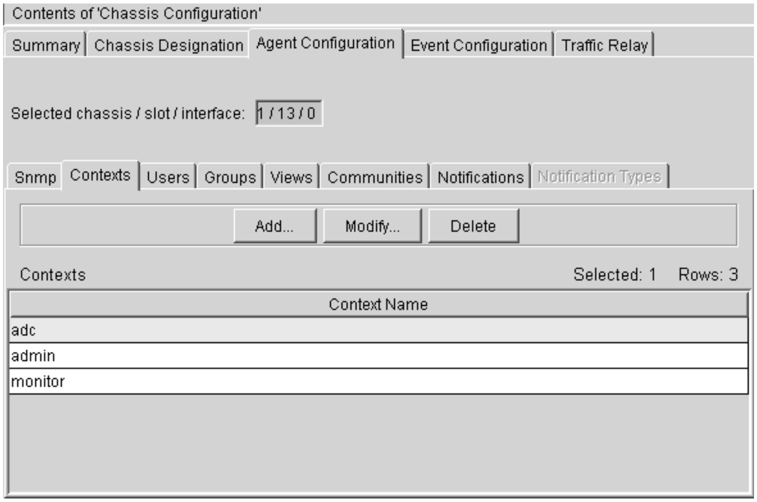
Database Status: Ok

Date	Type	Severity	Chassis/Slot/Interface	Description	Status
Sep 5, 2001 8:03:57 PM	DHCPRelay	Normal	113 / 9 / 0 / 1 - unauthorized	DHCP Relay Not Configured	Open
Sep 4, 2001 4:07:28 PM	Chassis Fault	Minor	113 / 13 / 0 / 1 - Power Supply AC	Chassis Fault	Open
Sep 4, 2001 2:33:35 PM	Chassis Fault	Minor	113 / 13 / 0 / 1 - Backplane Power A	Chassis Fault	Open
Sep 4, 2001 10:39:52 AM	ProvSrvc	Major	Server:-syslog daemon	CPM Service Event	Open
Sep 4, 2001 10:39:45 AM	SRVC	Normal	10 / 113 / 13 / 1 - ma	Software Up	Open

In the example above, a row must be selected in order to activate the available buttons.

For example, Figure 2-15 displays available buttons after the first row is selected. *Note the difference between Figure 2-15 and Figure 2-12.*

Figure 2-15 Example: Available Buttons.



Contents of 'Chassis Configuration'

Selected chassis / slot / interface: 1 / 13 / 0

Contexts Selected: 1 Rows: 3

Context Name
adc
admin
monitor

Topology View of the Cuda Network

The Cuda 12000 provides the ability to generate network diagrams. When you initially click the **Topology View** button from the desktop, the result is a display of the chassis group you have configured for the client chassis. Refer to Chapter 6, “Managing Multiple Chassis” on page 119, for information on accessing groups and multi-chassis in a group.

To expand the view, follow this procedure:

1. Click on a group symbol to view the chassis you have configured for the group. Refer to Figure 2-16.
2. Click on a chassis symbol to view its modules. Refer to Figure 2-17.
3. Click on a module symbol to view its attributes. Refer to Figure 2-18.

To expand or collapse a node for viewing the chassis within a group, click on the group symbol in the left panel. Figure 2-16 shows a network view expanded to show the chassis configured the Group named "Cuda." Notice that the chassis from which you are logged in is highlighted in beige.

Figure 2-16 Network View of Chassis in the Group "Cuda"

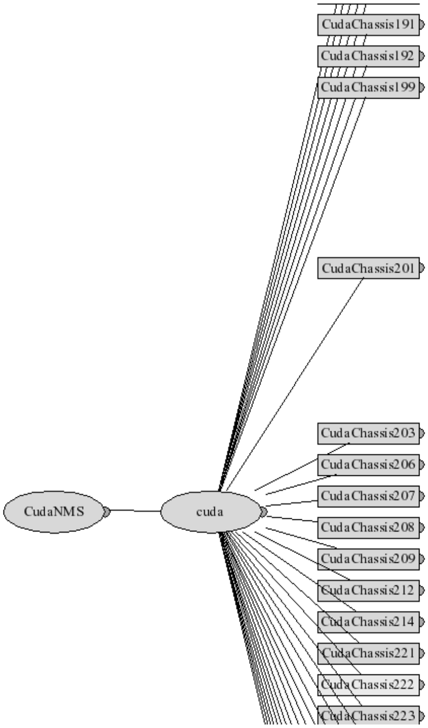


Figure 2-17 shows the available modules in the selected chassis including a CMTS module with its additional interfaces.

Figure 2-17 Module View

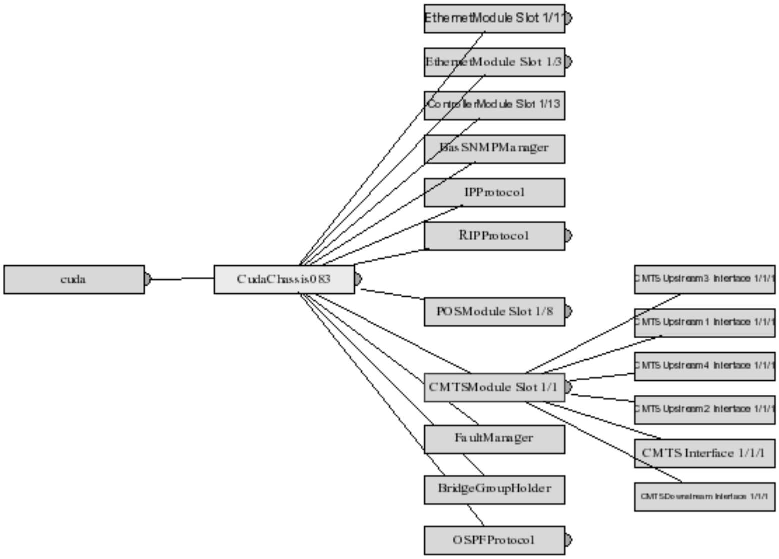
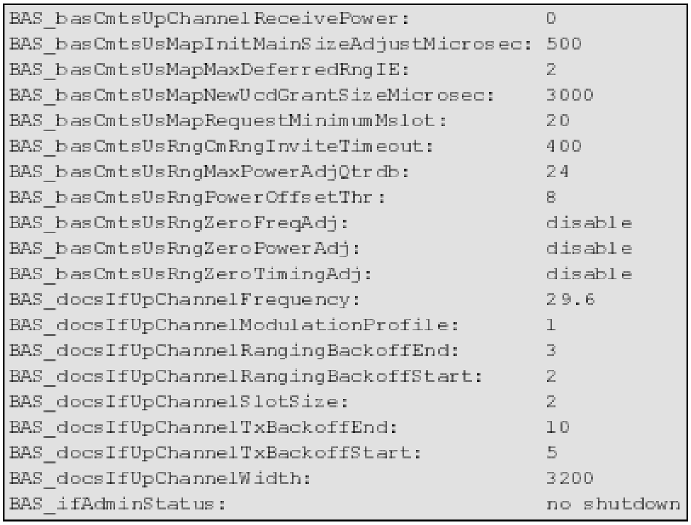


Figure 2-18 shows the attributes of a CMTS upstream 1 interface.

Figure 2-18 Module Attributes



```
BAS_basCmtsUpChannelReceivePower:          0
BAS_basCmtsUsMapInitMainSizeAdjustMicrosec: 500
BAS_basCmtsUsMapMaxDeferredRngIE:          2
BAS_basCmtsUsMapNewUcdGrantSizeMicrosec:    3000
BAS_basCmtsUsMapRequestMinimumMslot:       20
BAS_basCmtsUsRngCmRngInviteTimeout:        400
BAS_basCmtsUsRngMaxPowerAdjQtrdb:          24
BAS_basCmtsUsRngPowerOffsetThr:            8
BAS_basCmtsUsRngZeroFreqAdj:               disable
BAS_basCmtsUsRngZeroPowerAdj:              disable
BAS_basCmtsUsRngZeroTimingAdj:             disable
BAS_docsIfUpChannelFrequency:              29.6
BAS_docsIfUpChannelModulationProfile:      1
BAS_docsIfUpChannelRangingBackoffEnd:      3
BAS_docsIfUpChannelRangingBackoffStart:    2
BAS_docsIfUpChannelSlotSize:               2
BAS_docsIfUpChannelTxBackoffEnd:           10
BAS_docsIfUpChannelTxBackoffStart:         5
BAS_docsIfUpChannelWidth:                  3200
BAS_ifAdminStatus:                         no shutdown
```

Topology Control Menu

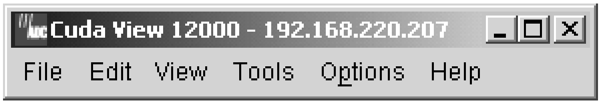
The Topology Control menu provides these buttons:

Button	Description
⟳	Refresh View
🔍 +	Zoom In
🔍 -	Zoom Out
▤▾	Expand all nodes for selected Cuda chassis
📁	Go back to top level group
✎	Remove all nodes

The Menu Bar

The Cuda 12000 offers a menu bar to help you manage your configuration. This section describes the menu commands supported by the Cuda 12000.

Figure 2-19 Desktop Menu Bar



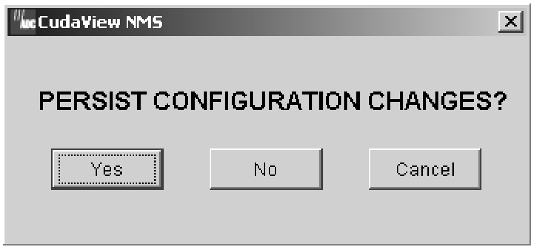
File Menu

The File menu supports these commands:

- **Save —** Saves the system configuration to the provisioning database, without exiting the desktop.
- **Exit —** Closes the desktop.

When you attempt to exit the desktop after making changes to the configuration, and you have not yet applied or saved the new configuration onto the provisioning database, then a prompt displays:

Figure 2-20 Persist Prompt Dialog Box



CudaView NMS

PERSIST CONFIGURATION CHANGES?

Persisting saves the configuration permanently.

Click **Yes** to persist and exit the desktop. Click **No** to exit the desktop without persisting configuration. Click **Cancel** to exit the dialog box without persisting the configuration.

Edit Menu

The Edit menu is currently not supported.

View Menu

The View menu supports this command:

- Memory — Displays the used, free, and total memory of the GUI editor in the java console.

Tools Menu

The Tools menu supports these commands:

- Bas Ping -- Sends Internet Control Message Protocol (ICMP) echo request packets to a node on your network to see if it is reachable and online.
- Trace Route --Allows you to trace the route that packets take from the Cuda 12000 to a destination. All arguments except the destination IP address are optional.
- Trace Log -- Allows you to monitor and view specific software-related information.

- CLI Console -- Allows you to execute CLI commands within the GUI. Refer to *CLI Cuda 12000 IP Access Switch CLI Reference Guide and Cuda 12000 IP Access Switch CLI-Based Administration Guide* for details.
- Enable Broadcast -- Enable or disable a broadcast by selecting Enable Broadcast. A broadcast message appears at the bottom of your window when you enable this option.

Refer to Chapter 3, “CudaView Desktop Tools” for information about these and other desktop tools.

Entering Configuration Information

Apply — When you enter new information in a configuration field, the new information does not take affect until you **Apply** the changes. To apply changes, click on the **Apply** button located on the same display. However, applied changes will be lost upon reboot if the changes are not persisted using the File/Save menu command.

Modifications — In most configuration windows throughout the system, when you make changes to a value, the field and the specific configuration tab turn blue, to indicate you have entered new information and have not yet applied the configuration.

3 CUDAVIEW DESKTOP TOOLS

This chapter describes the following desktop tools:

- Tools from the Tools menu
- Table Manipulation Tools
- Performance Graphing

Tools from the Tools Menu

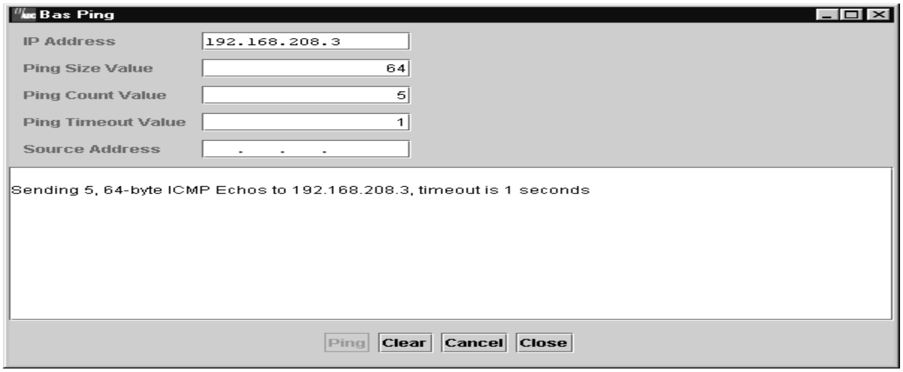
The Tools menu supports these functions. These functions are described in the appropriate sections that follow:

- Bas Ping
- Trace Route
- Trace Log
- CLI Console

Bas Ping

Use Bas Ping to send Internet Control Message Protocol (ICMP) echo request packets to a node on your network to see if it is reachable and online. The BAS Ping window appears:

Figure 3-1 BAS Ping Window



IP Address: 192.168.208.3
Ping Size Value: 64
Ping Count Value: 5
Ping Timeout Value: 1
Source Address: . . .

```
Sending 5, 64-byte ICMP Echos to 192.168.208.3, timeout is 1 seconds
```

Table 3-1 Parameters to be Configured for Pinging Packet

Parameters	Description
IP Address	Required — IP address of destination host that you want to ping.
Ping Size Value	Optional — Size of the ping to send. Valid range: 64 – 64000 bytes.
Ping Count Value	Optional — Number of pings to send. Valid range: 0 – 1000. A value of 0 means forever.

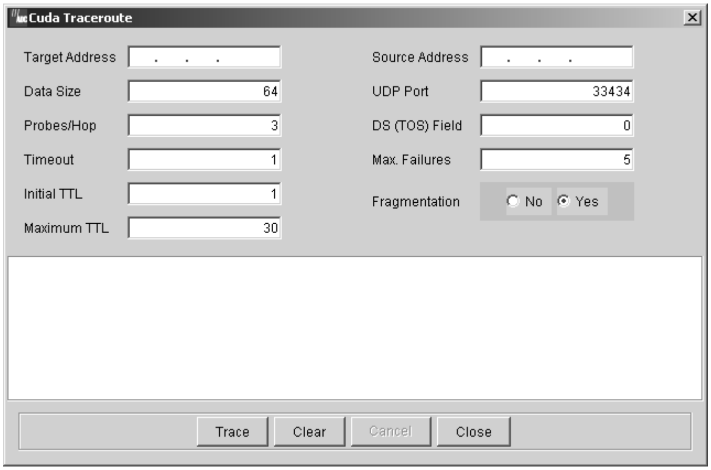
Parameters	Description
Ping Timeout Value	Optional — Number of seconds to wait for each reply. Valid range: 1 – 30.

Trace Route

Trace route allows you to trace the route that packets take from the Cuda 12000 to a destination. All arguments except the destination IP address are optional.

Before you use the trace route feature, ping the host you wish to reach. If you can reach the host, use the trace route feature to determine the route to the host.

Figure 3-2 Trace Route Window



Target Address	. . .	Source Address	. . .
Data Size	64	UDP Port	33434
Probes/Hop	3	DS (TOS) Field	0
Timeout	1	Max. Failures	5
Initial TTL	1	Fragmentation	○ No ● Yes
Maximum TTL	30		

Table 3-2 Trace Route Window Parameters.

Parameter	Description
Target Address	Destination IP address for the trace.
Data Size	Size, in bytes, of the probe packets in the trace. The values range from 64 to 64000 bytes. The default is 64.
Probes/Hops	Number of probe packets sent to each hop. The values range from 1 to 10. The default is 3.

Parameter	Description
Timeout	Number of seconds to wait for a response to a probe packet. The values range from 1 to 30. The default is 1. Note that a trace consists of a series of transmitted probe packets.
Intial TTL	Initial time-to-live (TTL) value in the number of hops, enabling you to bypass the initial (often well known) portion to a path. You can configure the trace to ignore hosts that are less than the specified number of hops away from your Cuda 12000. The values range from 0, indicating no initial TTL, to 255. The default is 1.
Maximum TTL	Maximum TTL value in the number of hops. When the Cuda 12000 send a trace route packet, the Cuda 12000 sets the TTL value in the packet to the value you specify. Each time a router forwards the packet, the router decrements this value by one. Routers discard packets that have a TTL to zero. Values range from 1 to 255. The default is 30.
Source Address	Source IP address in outgoing probe packets on the Cuda 12000. By default, the source IP address is the IP address of the interface that the Cuda 12000 sends the probe packet. If your Cuda 12000 has more than one IP address, this argument enables you to override the default source address.
UDP Port	Base UDP port number on the destination host that the trace route sends probe packets. Values range from 1 to 65535. The default is 33434. Trace route assumes that no other processes on the destination host use UDP port numbers in the range of base to base + nhops -1. For example, if the base is 33434, then the route uses a UDP port in the range: 33434 to 33434 + nhops -1 If another process listens on a port in this range, you can use this argument to specify a new base UDP port number, thereby configuring an unused port range.
DS (TOS) Field	Type-of-service (TOS) value in probe packets. The TOS field determines if different TOS values take different paths. Useful values are 16 (low delay) and 8 (high throughput). The value must be a decimal integer in the range from 0 to 255. The default is 0.

Parameter	Description
Max Failures	Maximum number of consecutive timeouts. The route stops the trace when this threshold is reached. The values range from 0 to 255. The default is 5.
Fragmentation	Disables or enables IP fragmentation for the trace. If you clear the check box to disable fragmentation, and the packet size that you specify with the data size parameter is so big that the routers fragment it along the route, the route indicates that fragmentation has occurred. If a router returns the value of the proper MTU size, the route decreases the packets size automatically to this new value. Otherwise, the route chooses a shorter packet size. By default, fragmentation is enabled.

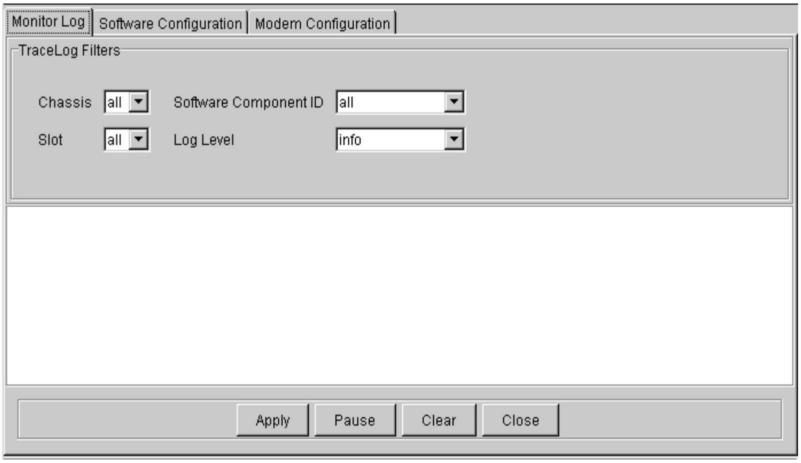
Trace Log

Trace Log allows you to monitor and view specific software-related information. You can use this information for performance monitoring, troubleshooting, and debugging purposes.

Within Trace Log, you are offered these configuration widows:

- Monitor Log
- Software Configuration
- Modem Configuration

Figure 3-3 Trace Log Configuration

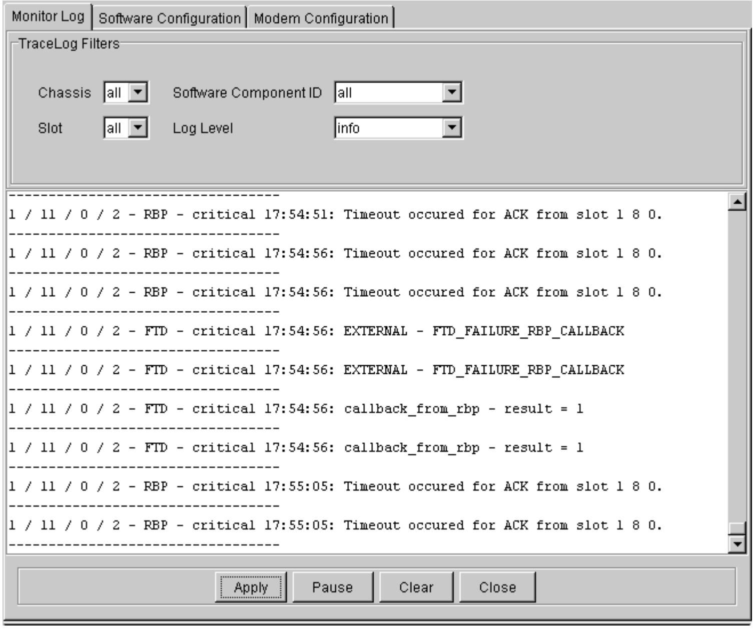


Chassis all
Software Component ID all
Slot all
Log Level info

Monitor Log — Allows you to choose specific views to display real-time trace log information. The view options are:

- Chassis — You can configure trace log information to view and monitor information on a chassis-wide basis.
- Slot — You can configure trace log information to view and monitor information on a slot-wide basis.
- Software Component ID — Specify the information *(in terms of software component ID)* that you want to monitor.
- Log Level — The trace logging severity level for the software component consisting of init, critical, warning, and info, which comprise all severity levels.

Figure 3-4 Monitor Log Tab

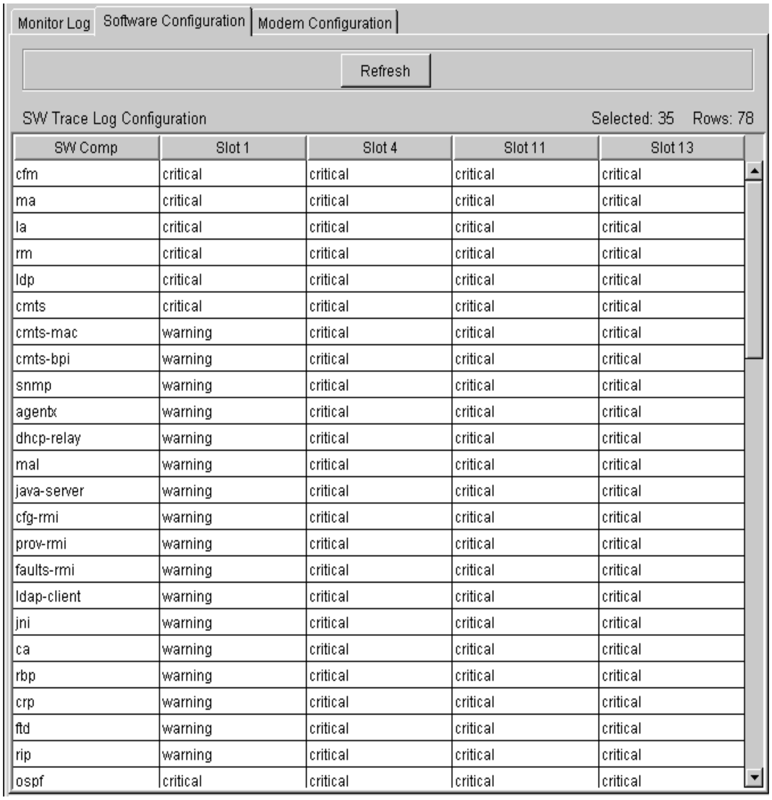


Chassis: all
Software Component ID: all
Slot: all
Log Level: info

```
----------------------------------
1 / 11 / 0 / 2 - RBP - critical 17:54:51: Timeout occured for ACK from slot 1 8 0.
----------------------------------
1 / 11 / 0 / 2 - RBP - critical 17:54:56: Timeout occured for ACK from slot 1 8 0.
----------------------------------
1 / 11 / 0 / 2 - RBP - critical 17:54:56: Timeout occured for ACK from slot 1 8 0.
----------------------------------
1 / 11 / 0 / 2 - FTD - critical 17:54:56: EXTERNAL - FTD_FAILURE_RBP_CALLBACK
----------------------------------
1 / 11 / 0 / 2 - FTD - critical 17:54:56: EXTERNAL - FTD_FAILURE_RBP_CALLBACK
----------------------------------
1 / 11 / 0 / 2 - FTD - critical 17:54:56: callback_from_rbp - result = 1
----------------------------------
1 / 11 / 0 / 2 - FTD - critical 17:54:56: callback_from_rbp - result = 1
----------------------------------
1 / 11 / 0 / 2 - RBP - critical 17:55:05: Timeout occured for ACK from slot 1 8 0.
----------------------------------
1 / 11 / 0 / 2 - RBP - critical 17:55:05: Timeout occured for ACK from slot 1 8 0.
----------------------------------
```

Software Configuration — Lists the sources of the software components that are supported by trace log.

Figure 3-5 Software Configuration Tab



SW Trace Log Configuration   Selected: 35   Rows: 78

SW Comp	Slot 1	Slot 4	Slot 11	Slot 13
cfm	critical	critical	critical	critical
ma	critical	critical	critical	critical
la	critical	critical	critical	critical
rm	critical	critical	critical	critical
ldp	critical	critical	critical	critical
cmts	critical	critical	critical	critical
cmts-mac	warning	critical	critical	critical
cmts-bpi	warning	critical	critical	critical
snmp	warning	critical	critical	critical
agentx	warning	critical	critical	critical
dhcp-relay	warning	critical	critical	critical
mal	warning	critical	critical	critical
java-server	warning	critical	critical	critical
cfg-rmi	warning	critical	critical	critical
prov-rmi	warning	critical	critical	critical
faults-rmi	warning	critical	critical	critical
ldap-client	warning	critical	critical	critical
jni	warning	critical	critical	critical
ca	warning	critical	critical	critical
rbp	warning	critical	critical	critical
crp	warning	critical	critical	critical
ftd	warning	critical	critical	critical
rip	warning	critical	critical	critical
ospf	critical	critical	critical	critical

Per slot you may choose a severity level of the software component trace, referred to as the log level. To set a log level, right click on the level that you want to set and choose one of the options, which are:

- init — includes init information
- critical — includes init and critical information
- warning — Includes init, critical, and warning information
- info — Includes init, critical, warning, and info information

We recommend that you do not select multiple log levels across slots at the same time. Selecting multiple levels affects processing performance.

Table 3-3 Software Components Supported by Trace Log

CFM - Configuration File Manager.	**FTD** - Events related to distributing the IP forwarding table.
MA - SNMP Master agent (slot 13 or 14 only)	**RIP** - *Not supported*.
LA - SNMP local agent on slots 1 - 12.	**IP** - *Not supported*.
rm	
LDP - Link Discover Protocol on slots 1 - 12	**OSPF** - *Not supported*.
CMTS - CMTS events other than MAC and BPI	**UDP** - *Not supported*.
CMTS_MAC - MAC only events	**TCP** - *Not supported*.
CMTS_BPI - Baseline Privacy events.	**SW** - *Not supported*.
SNMP - Events related to the SNMP protocol.	**ICMP** - *Not supported*.
AgentX - Events related to the agentx protocol between the master SNMP agent on the BCM and the and local agents on the I/O modules	**DHCP_SERVER** - DHCP Server events. Only valid on slots 13 and 14.
DHCP_RELAY - Events related to DHCP on an application module.	**TIME_SERVER** - Time Server events. Only valid on slots 13 and 14.
MAL - Management Access Layer which supports both CLI and GUI.	**SYSLOG_SERVER** - SYSLOG Server events. Only valid on slots 13 and 14.
JAVA_SERVER - Java server supporting the NMS and Provisioning GUI.	**TFTP_SERVER** - TFTP Server events. Only valid on slots 13 and 14.
CFG_RMI - Communications issues related to the configuration process.	**CLI** - Command Line Interface events. Only valid on slots 13 and 14.
PROV_RMI - Errors related to the provisioning server/GUI interaction.	**LOG** - log task.
FAULTS_RMI - Errors related to processing Alarms.	**TRACELOGD** - Tracelog Server events. Only valid on slots 13 and 14.
LDAP_CLIENT - Events related to the LDAP client.	**CMTS_GENERIC** - General CMTS events.
cmts-0 - Supported. For detailed information about this software component, contact customer service.	**cmts-1** - Supported. For detailed information about this software component, contact customer service.
cmts-2 - Supported. For detailed information about this software component, contact customer service.	**cmts-3** - Supported. For detailed information about this software component, contact customer service.

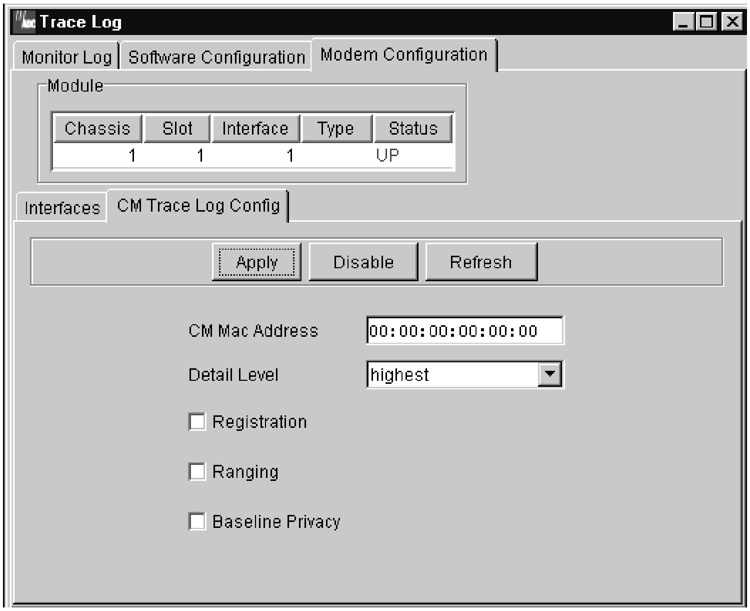
cmts-4 - Supported. For detailed information about this software component, contact customer service.	**cmts-5** - Supported. For detailed information about this software component, contact customer service.
cmts-6 - Supported. For detailed information about this software component, contact customer service.	**cmts-7** - Supported. For detailed information about this software component, contact customer service.
cmts-8 - Supported. For detailed information about this software component, contact customer service.	**cmts-9** - Supported. For detailed information about this software component, contact customer service.
cmts-10 - Supported. For detailed information about this software component, contact customer service.	**cmts-11** - Supported. For detailed information about this software component, contact customer service.
cmts-12 - Supported. For detailed information about this software component, contact customer service.	**cmts-13** - Supported. For detailed information about this software component, contact customer service.
cmts-14 - Supported. For detailed information about this software component, contact customer service.	**cmts-15** - Supported. For detailed information about this software component, contact customer service.
cmts-17 - Supported. For detailed information about this software component, contact customer service.	**rip-debug** - Supported. For detailed information about this software component, contact customer service.
JNI - Events related to the Java Network Interface.	**CMTS_DOCSIS_ERR** - DOCSIS specific errors.
CA - SNMP issues on the BCM.	**IDLE** - *Not supported*.
RBP - Events related to the ADC proprietary reliable IPC mechanism.	**RCV** - *Not supported*.
CRP - *Not supported*.	**RIP_MEM** - Events related to RIP memory allocation.
RIP_CONSOLE - Extensive debug of RIP, provides function level debugging. Developer debug only	**ROUTING_TRACE** - Trap based debugging for all routing protocols. Misconfigurations would be caught here.
IP_DEBUG - Extensive debug of IP, provides function level debugging. Developer debug only	**RIP_RX** - Events occurring during RIP receive packet handling.
RIP_TX - Events occurring during RIP transmission.	**RIP_TASK** - Events which occur within the main RIP task.
RIP_ROUTE - Events related to route updating.	**RIP_TIMER** - Events related to RIP periodic timers.

ppp-debug- Events related the LCP and IPCP messages used to establish the PPP link.	**ppp** - Events related the state of the PPP connection.
courier- *Not supported*.	**ospf-spf** - *Not supported*.
ospf-hello - *Not supported*.	**nlbg** - Events related to establishing the net layer bridge flow.
nlbg-rs - Distributes information to all modules regarding the nlbg interfaces.	**nlbg-cmts** - Enables tracking for nlbg database reception. Developer debug only.
RIP_STATE - Events related to internal RIP states.	**RIP_GENERAL** - Miscellaneous RIP events.

Modem Configuration — Allows you to configure trace log information to view and monitor cable modem-specific data on a per interface basis. Select the **Interfaces** tab and choose the interface.

- CM Trace Log Config — You can configure trace log information to view and monitor information as it pertains to the registration of a single cable modem. This allows you to view and monitor the information flow that occurs during a registration of a specific cable modem. Use this information to debug registration failures on a per cable modem basis. To configure trace log for a cable modem, perform these GUI operations in any order:
  - Specify the MAC address of the cable modem that you want to monitor.
  - Choose the detail level at which you want to monitor the specified information. The options are low, medium, high, and highest.
  - Select whether you want to monitor the cable modem registration messages.
  - Select whether you want to monitor cable ranging messages.
  - Select whether you want to monitor cable modem baseline privacy messages.

Figure 3-6 Modem Configuration Tab



Chassis	Slot	Interface	Type	Status
1	1	1		UP

CM Mac Address 00:00:00:00:00:00

Detail Level highest

□ Registration

□ Ranging

□ Baseline Privacy

Table 3-4 Modem Configuration Window Parameters

Enter values for these parameters:

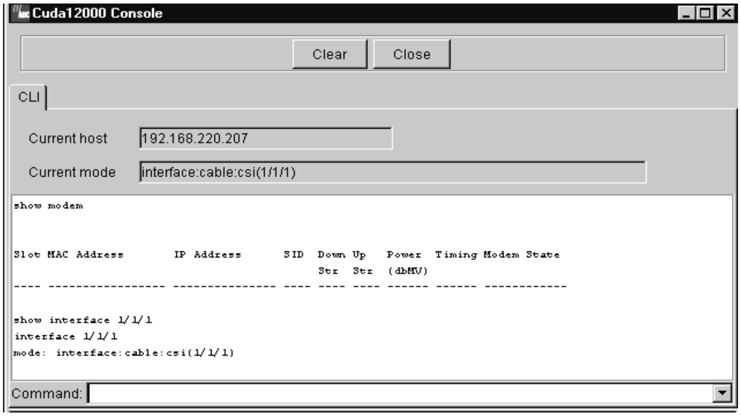
CM MAC Address	Specifies the MAC address of the modem that you want to monitor.
Detail Level	Specifies the level that you want to monitor the specified information.
Registration	Enables and disables the monitoring of messages that occur during the registration stage.
Ranging	Enables and disables the monitoring of messages that occur during the ranging stage.
Baseline Privacy	Enables and disables the monitoring of messages that occur during the baseline privacy stage *(applicable only when baseline privacy is enabled)*.

CLI Console

The CLI Console window allows you to execute CLI commands within the GUI.

When the Cuda 12000 Console appears, type the CLI command at the Command line. The current mode and output is displayed.

Figure 3-7 CLI Console



Current host 192.168.220.207

Current mode interface:cable:csi(1/1/1)

```
show modem


Slot MAC Address        IP Address      SID  Down Up   Power  Timing Modem State
                                             Str  Str  (dbMV)
---- ----------------- --------------- ---- ---- ---- ------ ------ ------------


show interface 1/1/1
interface 1/1/1
mode:  interface:cable:csi(1/1/1)
```

Table Manipulation

CudaView provides the ability to manipulate entries in lists and tables. The following is a list of options you may use to manipulate entries. These options are described in the appropriate sections that follow:

- Refresh
- Sort
- Search
- Performance Graphing

Refresh

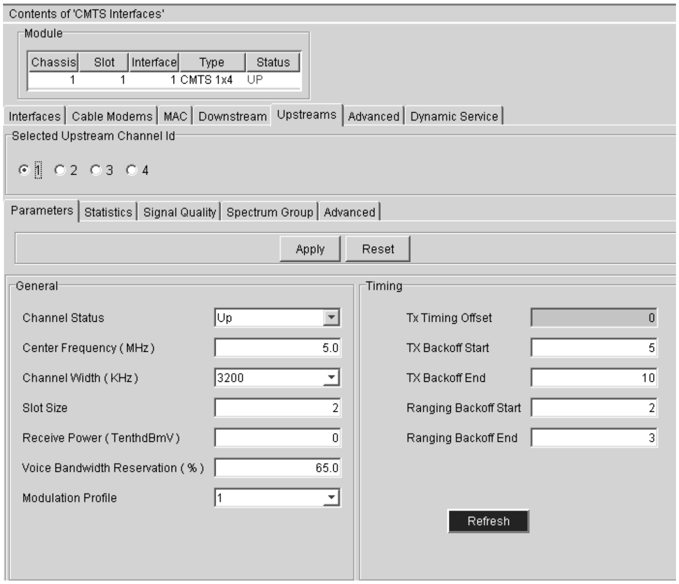
Refresh allows you to update parameter values with current status, statistics and configuration. You may update values by using one of the following procedures:

- Click the **Refresh** button, which is located in the top-half of a window.
- Use the context-sensitive right-click feature.

To update values using the context-sensitive right-click feature, follow this procedure:

1. From a list or table window, right-click anywhere in the window.
2. Click **Refresh**. The parameters are updated with current information.

Figure 3-8 Refresh Option



Contents of 'CMTS Interfaces'

Module

Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

General

Channel Status	Up
Center Frequency (MHz)	5.0
Channel Width (KHz)	3200
Slot Size	2
Receive Power (TenthdBmV)	0
Voice Bandwidth Reservation (%)	65.0
Modulation Profile	1

Timing

Tx Timing Offset	0
TX Backoff Start	5
TX Backoff End	10
Ranging Backoff Start	2
Ranging Backoff End	3

Sort

Sort allows you to reorder table column entries in ascending or descending order. You may sort columns by using one of the following procedures:

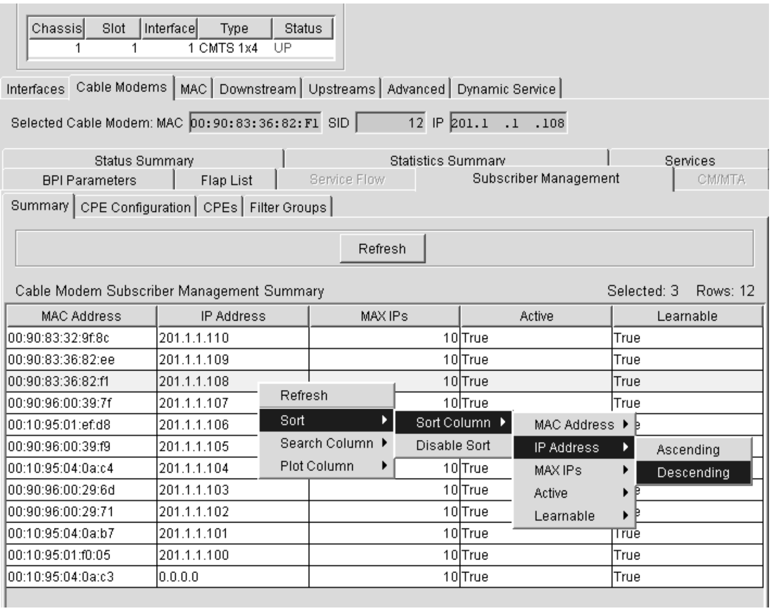
- Place the cursor on a column heading and click either the left or right mouse button.
- Use the context-sensitive right-click feature.

To sort a column by using the context-sensitive right-click feature, follow this procedure:

1. Select a column to sort. Left-click anywhere in the specific column. The entire row is shaded blue.
2. Right-click to open the sort tool.
3. Navigate the cursor over the sort options and sub-menus as follows: **Sort** > **Sort Column** > *Desired_Column*.
4. Left-click to choose Ascending or Descending. The column is updated to the selected order.

In Figure 3-9, “Sort Menu and Sub-Menus”, the "IP Address" column is selected and sorted in descending order.

Figure 3-9 Sort Menu and Sub-Menus



Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

Selected Cable Modem: MAC 00:90:83:36:82:F1 SID 12 IP 201.1 .1 .108

Cable Modem Subscriber Management Summary Selected: 3 Rows: 12

MAC Address	IP Address	MAX IPs	Active	Learnable
00:90:83:32:9f:8c	201.1.1.110	10	True	True
00:90:83:36:82:ee	201.1.1.109	10	True	True
00:90:83:36:82:f1	201.1.1.108	10	True	True
00:90:96:00:39:7f	201.1.1.107	10	True	True
00:10:95:01:ef:d8	201.1.1.106			e
00:90:96:00:39:f9	201.1.1.105			
00:10:95:04:0a:c4	201.1.1.104	10	True	
00:90:96:00:29:6d	201.1.1.103	10	True	
00:90:96:00:29:71	201.1.1.102	10	True	e
00:10:95:04:0a:b7	201.1.1.101	10	True	True
00:10:95:01:f0:05	201.1.1.100	10	True	True
00:10:95:04:0a:c3	0.0.0.0	10	True	True

Disabling and Enabling Sort

You may disable and enable the sort option for the table, using the context-sensitive right-click feature.

To disable sort; follow this procedure:

1. Left-click anywhere in the table. The entire row is shaded blue.
2. Right-click to open the sort tool.
3. Choose **Disable Sort**.

To enable sort, follow the steps as described in the previous section "Sort."

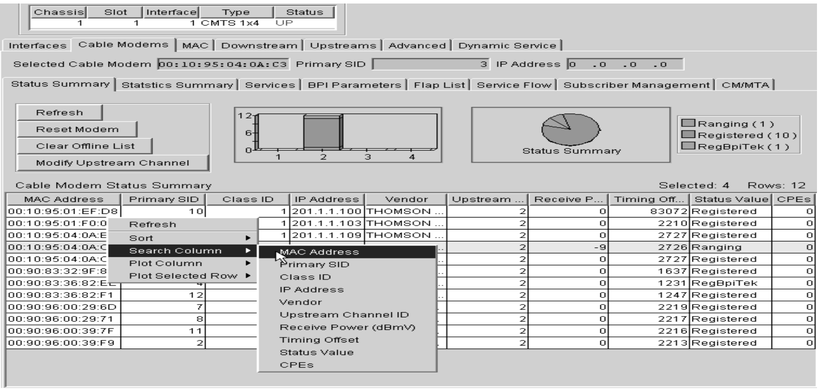
Search

Search allows you to find a specific table entry within a column.

To search for an entry, follow this procedure:

1. Place the cursor anywhere in the table and right-click to open the search tool.
2. Navigate the search option and sub-menus as follows: **Search Column>***Desired_Column*. Refer to Figure 3-10.
3. Select the column that you want to search. The **Find In Column:** *Column Name* dialog box appears.
4. In the "Find What" field, enter the value or text that you want to find and select the search criteria. Refer to Figure 3-11.
5. Click **Find Next** to begin the search; or click **Cancel** to exit without searching.

Figure 3-10 Search Column Menu and Sub-Menu



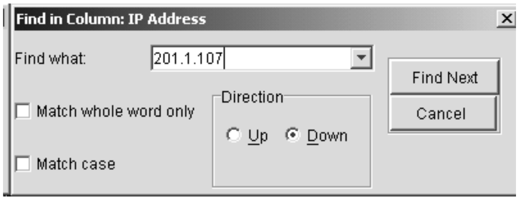
Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

Selected Cable Modem 00:10:95:04:0A:C3 Primary SID 3 IP Address 0 .0 .0 .0

Cable Modem Status Summary Selected: 4 Rows: 12

MAC Address	Primary SID	Class ID	IP Address	Vendor	Upstream ...	Receive P...	Timing Off...	Status Value	CPEs
00:10:95:01:EF:D8	10	1	201.1.1.100	THOMSON ...	2	0	83072	Registered	0
00:10:95:01:F0:0		1	201.1.1.103	THOMSON ...	2	0	2210	Registered	0
00:10:95:04:0A:E		1	201.1.1.109	THOMSON ...	2	0	2727	Registered	0
00:10:95:04:0A:C				...	2	-9	2726	Ranging	0
00:10:95:04:0A:C				...	2	0	2727	Registered	0
00:90:83:32:9F:8				...	2	0	1637	Registered	0
00:90:83:36:82:E	4			...	2	0	1231	RegBpiTek	0
00:90:83:36:82:F1	12			...	2	0	1247	Registered	0
00:90:96:00:29:6D	7				2	0	2219	Registered	0
00:90:96:00:29:71	8				2	0	2217	Registered	0
00:90:96:00:39:7F	11				2	0	2216	Registered	0
00:90:96:00:39:F9	2				2	0	2213	Registered	0

Figure 3-11 Search Dialog Box



Find in Column: IP Address

Find what: 201.1.107

☐ Match whole word only

☐ Match case

Direction ○ Up ● Down

Performance Graphing

Performance Graphing supports histogram and real-time plotting of various statistics counters and utilization of the Cuda 12000 operations.

This tool produces three types of graphs:

- A bar chart, whose source is statistical data from a table.
- A pie chart, whose source is textual data table.
- A line chart, whose source is:
  - real-time statistics at a specified time interval
  - statistical data from tables and list-type windows

Plotting

The Cuda 12000 supports plotting, by using the context-sensitive right-click feature. You may create bar and pie charts using data from a selected table column and all table columns. You may create real-time line charts using statistical data from a selected table row, and statistical data from list-type windows.

Plotting a Bar Graph

You may plot a bar graph from using data from all table columns, or from using statistical data from a selected table column.

To plot a bar graph from all columns or a selected column, follow this procedure:

1. Right-click anywhere on the table, to open the plotting options.
2. Navigate the cursor to **Plot Column**.
3. Choose the following:

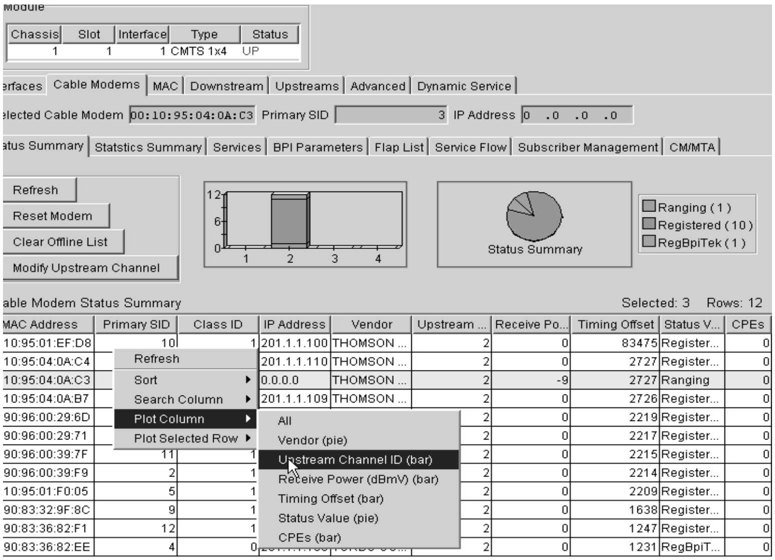
   a. All to plot data from all columns. *(Note: **All** produces both bar and pie graphs for all columns.)*;

   b.*Desired_Column (bar)* to plot statistical data from a selected table column.

Example 1

Figure 3-12 is an example of choosing a selected table column to plot a bar graph. Figure 3-13 is the bar graph of a selected table column.

Figure 3-12 Plot Column Menu and Sub-Menu with Upstream Channel ID Selected.



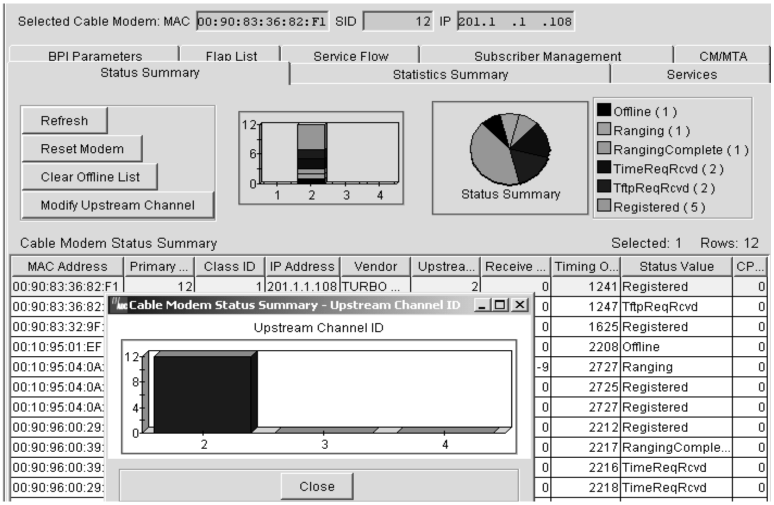
Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

elected Cable Modem 00:10:95:04:0A:C3 Primary SID 3 IP Address 0 .0 .0 .0

able Modem Status Summary Selected: 3 Rows: 12

MAC Address	Primary SID	Class ID	IP Address	Vendor	Upstream ...	Receive Po...	Timing Offset	Status V...	CPEs
10:95:01:EF:D8	10	1	201.1.1.100	THOMSON ...	2	0	83475	Register...	0
10:95:04:0A:C4			201.1.1.110	THOMSON ...	2	0	2727	Register...	0
10:95:04:0A:C3			0.0.0.0	THOMSON ...	2	-9	2727	Ranging	0
10:95:04:0A:B7			201.1.1.109	THOMSON ...	2	0	2726	Register...	0
90:96:00:29:6D					2	0	2219	Register...	0
90:96:00:29:71					2	0	2217	Register...	0
90:96:00:39:7F	11	1			2	0	2215	Register...	0
90:96:00:39:F9	2	1			2	0	2214	Register...	0
10:95:01:F0:05	5	1			2	0	2209	Register...	0
90:83:32:9F:8C	9	1			2	0	1638	Register...	0
90:83:36:82:F1	12	1			2	0	1247	Register...	0
90:83:36:82:EE	4	0			2	0	1231	RegBpiT...	0

Figure 3-13 Upstream Channel ID (Histogram)



Selected Cable Modem: MAC 00:90:83:36:82:F1 SID 12 IP 201.1 .1 .108

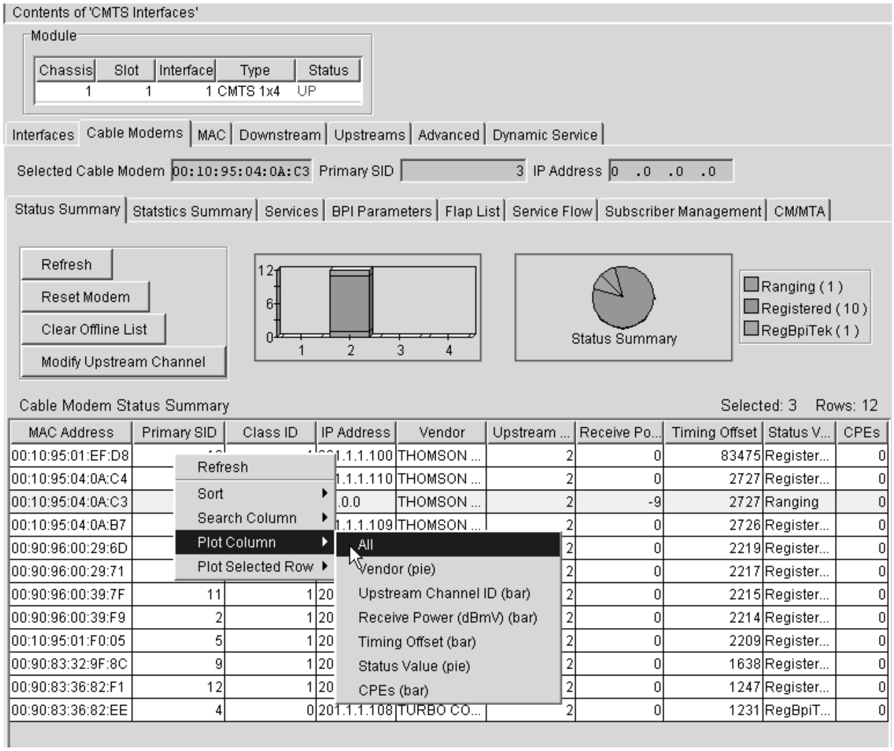
Cable Modem Status Summary Selected: 1 Rows: 12

MAC Address	Primary ...	Class ID	IP Address	Vendor	Upstrea...	Receive ...	Timing O...	Status Value	CP...
00:90:83:36:82:F1	12	1	201.1.1.108	TURBO ...	2	0	1241	Registered	0
00:90:83:36:82:						0	1247	TftpReqRcvd	0
00:90:83:32:9F:						0	1625	Registered	0
00:10:95:01:EF						0	2208	Offline	0
00:10:95:04:0A:						-9	2727	Ranging	0
00:10:95:04:0A:						0	2725	Registered	0
00:10:95:04:0A:						0	2727	Registered	0
00:90:96:00:29:						0	2212	Registered	0
00:90:96:00:39:						0	2217	RangingComple...	0
00:90:96:00:39:						0	2216	TimeReqRcvd	0
00:90:96:00:29:						0	2218	TimeReqRcvd	0

Example 2

Figure 3-14 is an example of choosing all table columns to plot bar and pie graphs. Figure 3-15 displays the graphs of all table columns.

Figure 3-14 Plot Column Menu and Sub-Menu with All Selected



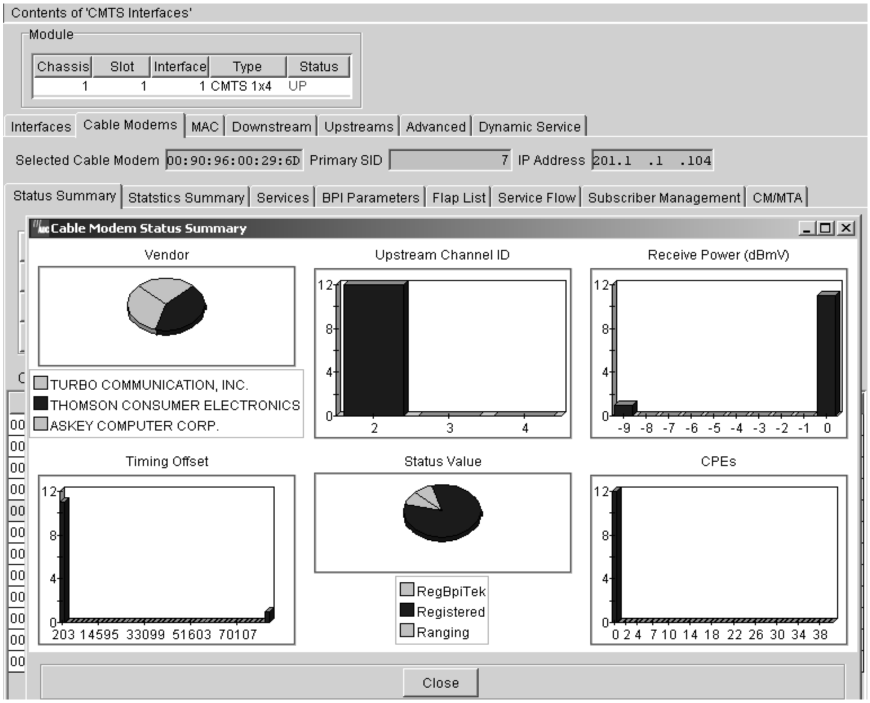
Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

Selected Cable Modem 00:10:95:04:0A:C3 Primary SID 3 IP Address 0 .0 .0 .0

Cable Modem Status Summary Selected: 3 Rows: 12

MAC Address	Primary SID	Class ID	IP Address	Vendor	Upstream ...	Receive Po...	Timing Offset	Status V...	CPEs
00:10:95:01:EF:D8			1.1.1.100	THOMSON ...	2	0	83475	Register...	0
00:10:95:04:0A:C4			1.1.1.110	THOMSON ...	2	0	2727	Register...	0
00:10:95:04:0A:C3			.0.0	THOMSON ...	2	-9	2727	Ranging	0
00:10:95:04:0A:B7			1.1.1.109	THOMSON ...	2	0	2726	Register...	0
00:90:96:00:29:6D					2	0	2219	Register...	0
00:90:96:00:29:71					2	0	2217	Register...	0
00:90:96:00:39:7F	11	1	20		2	0	2215	Register...	0
00:90:96:00:39:F9	2	1	20		2	0	2214	Register...	0
00:10:95:01:F0:05	5	1	20		2	0	2209	Register...	0
00:90:83:32:9F:8C	9	1	20		2	0	1638	Register...	0
00:90:83:36:82:F1	12	1	20		2	0	1247	Register...	0
00:90:83:36:82:EE	4	0	201.1.1.108	TURBO CO...	2	0	1231	RegBpiT...	0

Figure 3-15 All Table Columns Plotted



Contents of 'CMTS Interfaces'

Module

Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

Selected Cable Modem 00:90:96:00:29:6D Primary SID 7 IP Address 201.1 .1 .104

Plotting a Pie Graph

You may plot a pie graph from using textual data from a selected table column.

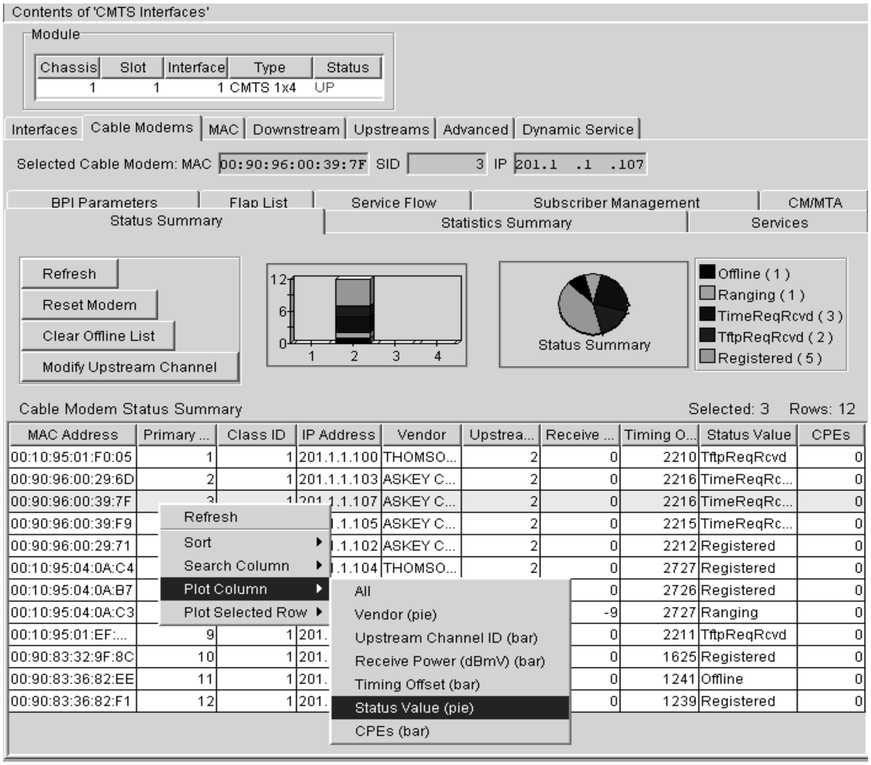
To plot a pie graph from a selected table column, follow this procedure:

1. Right-click anywhere on the table, to open the plotting options.
2. Navigate the cursor to **Plot Column**.
3. Choose *Desired_Column (pie)* to plot textual data from a selected table column.

Example

Figure 3-16 is an example of choosing a selected table column to plot a pie graph. Figure 3-17 is the pie graph of textual data.

Figure 3-16 Plot Column Menu and Sub-Menu with Status Value Column Selected



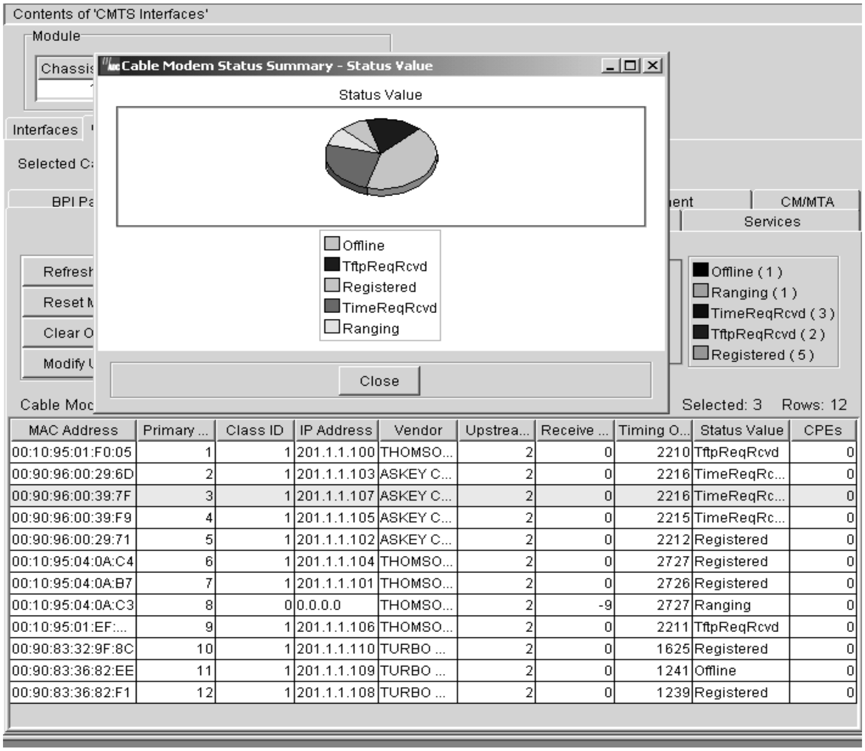
Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

Selected Cable Modem: MAC 00:90:96:00:39:7F SID 3 IP 201.1 .1 .107

Cable Modem Status Summary Selected: 3 Rows: 12

MAC Address	Primary ...	Class ID	IP Address	Vendor	Upstrea...	Receive ...	Timing O...	Status Value	CPEs
00:10:95:01:F0:05	1	1	201.1.1.100	THOMSO...	2	0	2210	TftpReqRcvd	0
00:90:96:00:29:6D	2	1	201.1.1.103	ASKEY C...	2	0	2216	TimeReqRc...	0
00:90:96:00:39:7F	3	1	201.1.1.107	ASKEY C...	2	0	2216	TimeReqRc...	0
00:90:96:00:39:F9			.1.1.105	ASKEY C...	2	0	2215	TimeReqRc...	0
00:90:96:00:29:71			.1.1.102	ASKEY C...	2	0	2212	Registered	0
00:10:95:04:0A:C4			.1.1.104	THOMSO...	2	0	2727	Registered	0
00:10:95:04:0A:B7						0	2726	Registered	0
00:10:95:04:0A:C3						-9	2727	Ranging	0
00:10:95:01:EF:...	9	1	201.			0	2211	TftpReqRcvd	0
00:90:83:32:9F:8C	10	1	201.			0	1625	Registered	0
00:90:83:36:82:EE	11	1	201.			0	1241	Offline	0
00:90:83:36:82:F1	12	1	201.			0	1239	Registered	0

Figure 3-17 Status Value Pie Graph



MAC Address	Primary ...	Class ID	IP Address	Vendor	Upstrea...	Receive ...	Timing O...	Status Value	CPEs
00:10:95:01:F0:05	1	1	201.1.1.100	THOMSO...	2	0	2210	TftpReqRcvd	0
00:90:96:00:29:6D	2	1	201.1.1.103	ASKEY C...	2	0	2216	TimeReqRc...	0
00:90:96:00:39:7F	3	1	201.1.1.107	ASKEY C...	2	0	2216	TimeReqRc...	0
00:90:96:00:39:F9	4	1	201.1.1.105	ASKEY C...	2	0	2215	TimeReqRc...	0
00:90:96:00:29:71	5	1	201.1.1.102	ASKEY C...	2	0	2212	Registered	0
00:10:95:04:0A:C4	6	1	201.1.1.104	THOMSO...	2	0	2727	Registered	0
00:10:95:04:0A:B7	7	1	201.1.1.101	THOMSO...	2	0	2726	Registered	0
00:10:95:04:0A:C3	8	0	0.0.0.0	THOMSO...	2	-9	2727	Ranging	0
00:10:95:01:EF:...	9	1	201.1.1.106	THOMSO...	2	0	2211	TftpReqRcvd	0
00:90:83:32:9F:8C	10	1	201.1.1.110	TURBO ...	2	0	1625	Registered	0
00:90:83:36:82:EE	11	1	201.1.1.109	TURBO ...	2	0	1241	Offline	0
00:90:83:36:82:F1	12	1	201.1.1.108	TURBO ...	2	0	1239	Registered	0

Plotting Real-time Line Graphs

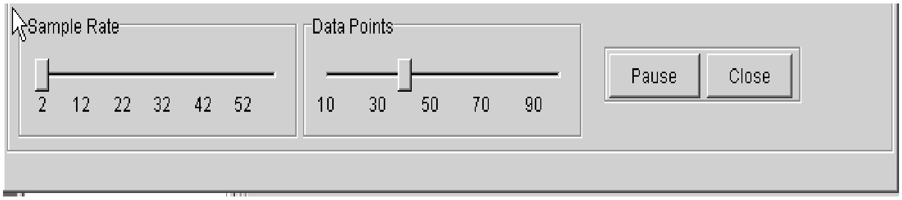
The Cuda 12000 supports real-time line graphing for statistical data. You may produce line graphs from the following data sources:

- Statistical data from the entire table or a selected row.
- Statistical data from a list-type window

The "X" axis of the line graph indicates time interval data points.

Using the data control panel within a graph, you may specify the sample rates and data points that you want to plot. To specify sample rates and data points, slide the bar to the desired points. Refer to Figure 3-18.

Figure 3-18 Real-time Data Control Panel



Parameter Descriptions

This table describes the parameters of the data control panel.

Table 3-5 Data Control Panel Parameters

Data Control	Description
Sample Rate	Contols the sampling rate. Data is sampled at approximately every two seconds. You may sample data for up to 52 seconds.
Data Points	Controls the number of data points to be plotted. You may plot up to 90 data points.
Pause/Resume	A toggle button used to freeze and restart the plotting.
Close	Exit out of the graph.

Plotting a Real-time Line Graph from a Table

To plot a line graph of all statistical data in a table or a selected table row, follow this procedure:

1. Right-click anywhere on the table, to open the plotting options.

2. Navigate the cursor to **Plot Selected Row**.

3. Choose the following:

a. All to plot statistical data from the entire table;

b.*Desired_Data* to plot statistical data for a selected row.

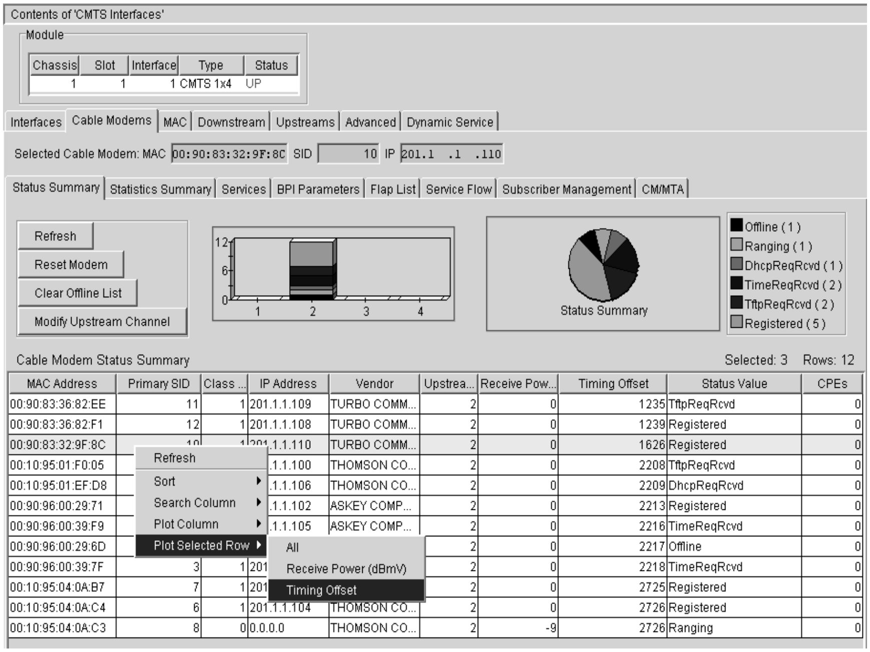
4. Select the Sample Rate and Data Points that you want to plot. Refer to Figure 3-20.

5. Click **Pause** to freeze the plotting, and click **Resume** to re-start the plotting.
6. Click **Close** to exit the graph window.

Example 1

Figure 3-19 is an example of choosing a selected row to plot a real-time line graph. Figure 3-20 is the line graph of a selected row.

Figure 3-19 Plot Selected Row Menu and Sub-Menu with Timing Offset Selected



Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

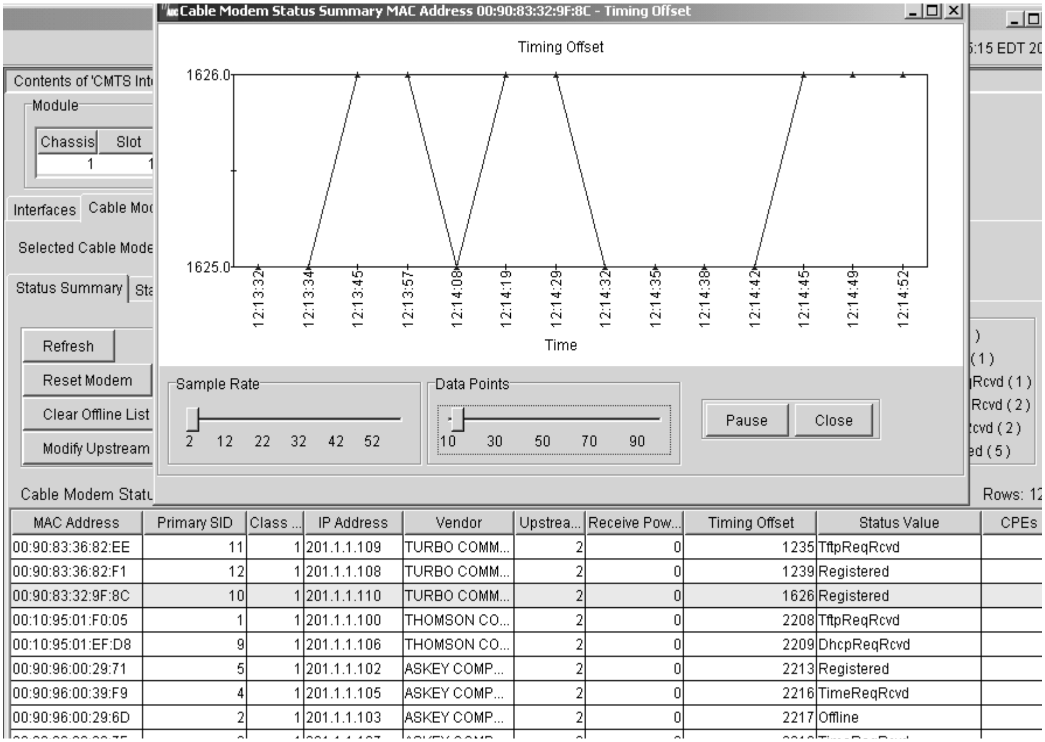
Selected Cable Modem: MAC 00:90:83:32:9F:8C SID 10 IP 201.1 .1 .110

Cable Modem Status Summary

Selected: 3 Rows: 12

MAC Address	Primary SID	Class ...	IP Address	Vendor	Upstrea...	Receive Pow...	Timing Offset	Status Value	CPEs
00:90:83:36:82:EE	11	1	201.1.1.109	TURBO COMM...	2	0	1235	TftpReqRcvd	0
00:90:83:36:82:F1	12	1	201.1.1.108	TURBO COMM...	2	0	1239	Registered	0
00:90:83:32:9F:8C	10	1	201.1.1.110	TURBO COMM...	2	0	1626	Registered	0
00:10:95:01:F0:05			.1.1.100	THOMSON CO...	2	0	2208	TftpReqRcvd	0
00:10:95:01:EF:D8			.1.1.106	THOMSON CO...	2	0	2209	DhcpReqRcvd	0
00:90:96:00:29:71			.1.1.102	ASKEY COMP...	2	0	2213	Registered	0
00:90:96:00:39:F9			.1.1.105	ASKEY COMP...	2	0	2216	TimeReqRcvd	0
00:90:96:00:29:6D					2	0	2217	Offline	0
00:90:96:00:39:7F	3	1	201		2	0	2218	TimeReqRcvd	0
00:10:95:04:0A:B7	7	1	201		2	0	2725	Registered	0
00:10:95:04:0A:C4	6	1	201.1.1.104	THOMSON CO...	2	0	2726	Registered	0
00:10:95:04:0A:C3	8	0	0.0.0.0	THOMSON CO...	2	-9	2726	Ranging	0

Figure 3-20 Real-time line chart of Timing Offset

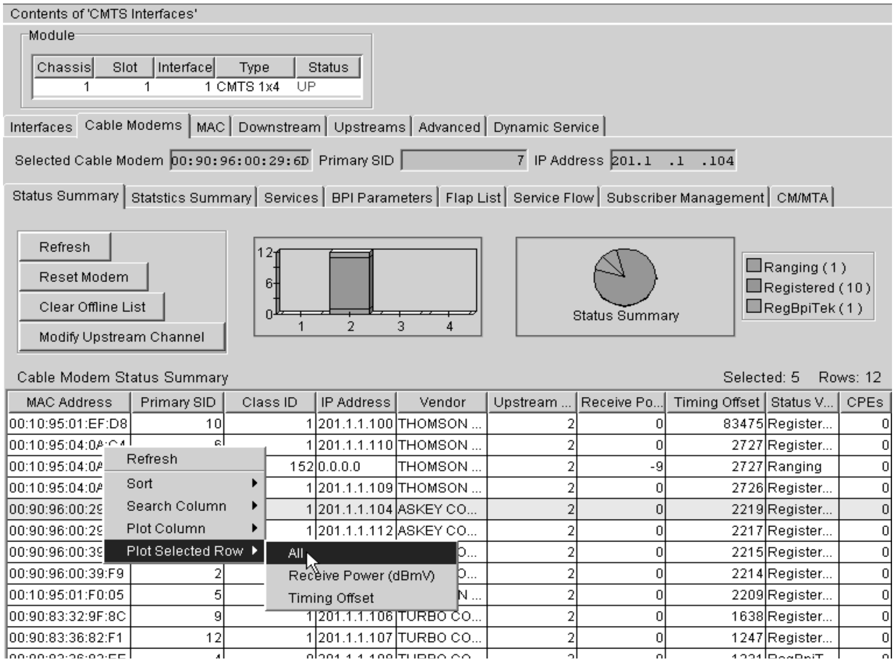


MAC Address	Primary SID	Class ...	IP Address	Vendor	Upstrea...	Receive Pow...	Timing Offset	Status Value	CPEs
00:90:83:36:82:EE	11	1	201.1.1.109	TURBO COMM...	2	0	1235	TftpReqRcvd	
00:90:83:36:82:F1	12	1	201.1.1.108	TURBO COMM...	2	0	1239	Registered	
00:90:83:32:9F:8C	10	1	201.1.1.110	TURBO COMM...	2	0	1626	Registered	
00:10:95:01:F0:05	1	1	201.1.1.100	THOMSON CO...	2	0	2208	TftpReqRcvd	
00:10:95:01:EF:D8	9	1	201.1.1.106	THOMSON CO...	2	0	2209	DhcpReqRcvd	
00:90:96:00:29:71	5	1	201.1.1.102	ASKEY COMP...	2	0	2213	Registered	
00:90:96:00:39:F9	4	1	201.1.1.105	ASKEY COMP...	2	0	2216	TimeReqRcvd	
00:90:96:00:29:6D	2	1	201.1.1.103	ASKEY COMP...	2	0	2217	Offline	

Example 2

Figure 3-21 is an example of choosing all statistical data in a table to plot a real-time line graph. Figure 3-22 is the line graph of all statistical data in a table.

Figure 3-21 Plot Menu and Sub-menu with All Selected



Contents of 'CMTS Interfaces'

Module

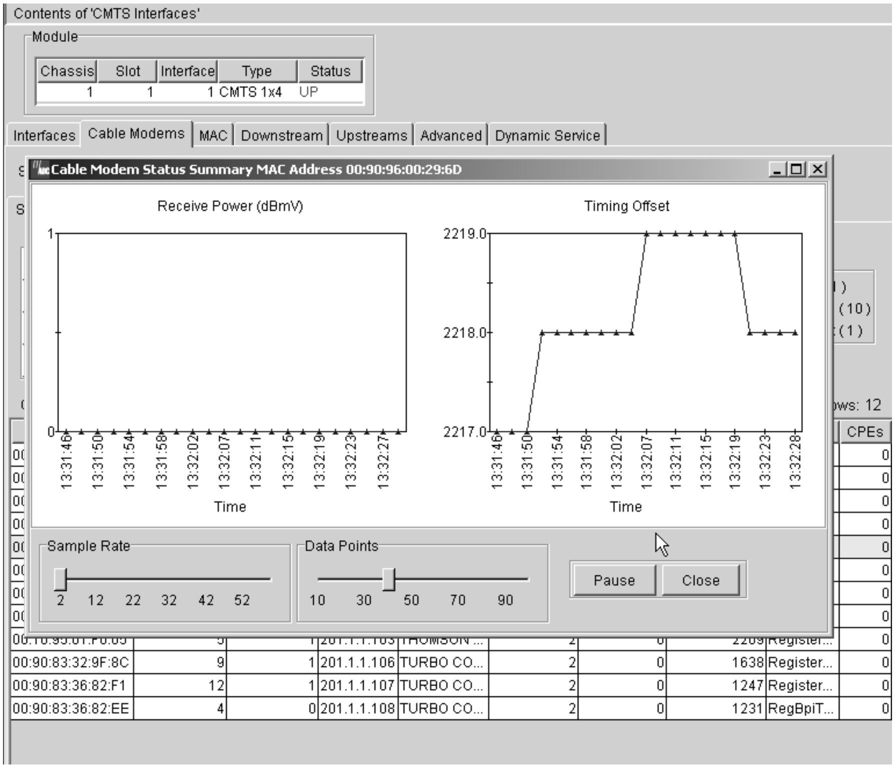
Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

Selected Cable Modem 00:90:96:00:29:6D Primary SID 7 IP Address 201.1 .1 .104

Cable Modem Status Summary Selected: 5 Rows: 12

MAC Address	Primary SID	Class ID	IP Address	Vendor	Upstream ...	Receive Po...	Timing Offset	Status V...	CPEs
00:10:95:01:EF:D8	10	1	201.1.1.100	THOMSON ...	2	0	83475	Register...	0
00:10:95:04:0A:C4	6	1	201.1.1.110	THOMSON ...	2	0	2727	Register...	0
00:10:95:04:0A		152	0.0.0.0	THOMSON ...	2	-9	2727	Ranging	0
00:10:95:04:0A		1	201.1.1.109	THOMSON ...	2	0	2726	Register...	0
00:90:96:00:29		1	201.1.1.104	ASKEY CO...	2	0	2219	Register...	0
00:90:96:00:29		1	201.1.1.112	ASKEY CO...	2	0	2217	Register...	0
00:90:96:00:39				O...	2	0	2215	Register...	0
00:90:96:00:39:F9	2			O...	2	0	2214	Register...	0
00:10:95:01:F0:05	5			N ...	2	0	2209	Register...	0
00:90:83:32:9F:8C	9	1	201.1.1.106	TURBO CO...	2	0	1638	Register...	0
00:90:83:36:82:F1	12	1	201.1.1.107	TURBO CO...	2	0	1247	Register...	0

Figure 3-22 Real-time Line Graph of All Statistical Values Plotted



Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

00:10:95:01:F0:05	5	1	201.1.1.103	THOMSON ...	2	0	2209	Register...	0
00:90:83:32:9F:8C	9	1	201.1.1.106	TURBO CO...	2	0	1638	Register...	0
00:90:83:36:82:F1	12	1	201.1.1.107	TURBO CO...	2	0	1247	Register...	0
00:90:83:36:82:EE	4	0	201.1.1.108	TURBO CO...	2	0	1231	RegBpiT...	0

Plotting Real-time Line Graphs for a List-type Window

You may plot a real-time line graph from a list-type window, of all statistical data or a selected parameter.

To plot a line graph of all statistical data or a selected parameter, follow this procedure:

1. Right-click in the list-type window, except within the value fields.
2. Navigate the cursor to **Plot**.
3. Choose the following:

   a. All to plot statistical data from the entire window;

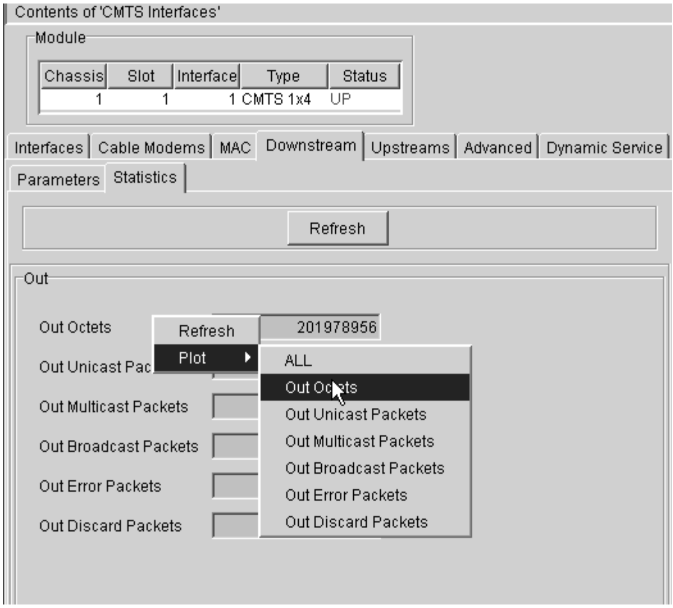
   b.*Desired_Data* to plot statistical data for a selected parameter.

4. Select the Sample Rate and Data Points that you want to plot. Refer to Figure 3-24.
5. Click **Pause** to freeze the plotting, and click **Resume** to re-start the plotting.
6. Click **Close** to exit the graph window.

Example 1

Figure 3-23 is an example of choosing a specific parameter to produce a line graph. Figure 3-24 is an example the line graph for a specific parameter.

Figure 3-23 Plot Menu and Sub-menu with Out Octets Parameter Selected.



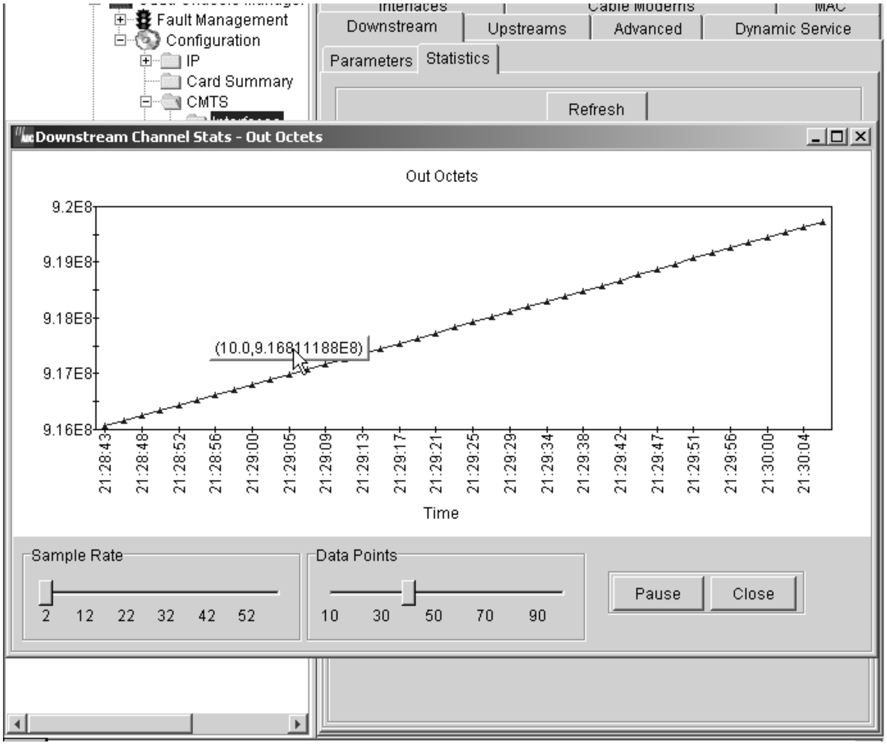
Contents of 'CMTS Interfaces'

Module

Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

Out Octets 201978956

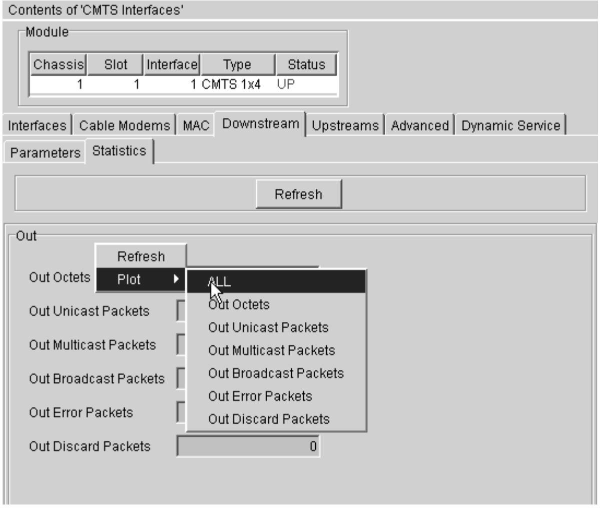
Figure 3-24 Real-time Plot of Out Octets Parameter



Example 2

Figure 3-25 is an example of choosing all parameters to produce a line graph. Figure 3-26 is an example of the line graph for all parameters.

Figure 3-25 Plot Menu and Sub-menu with ALL Selected



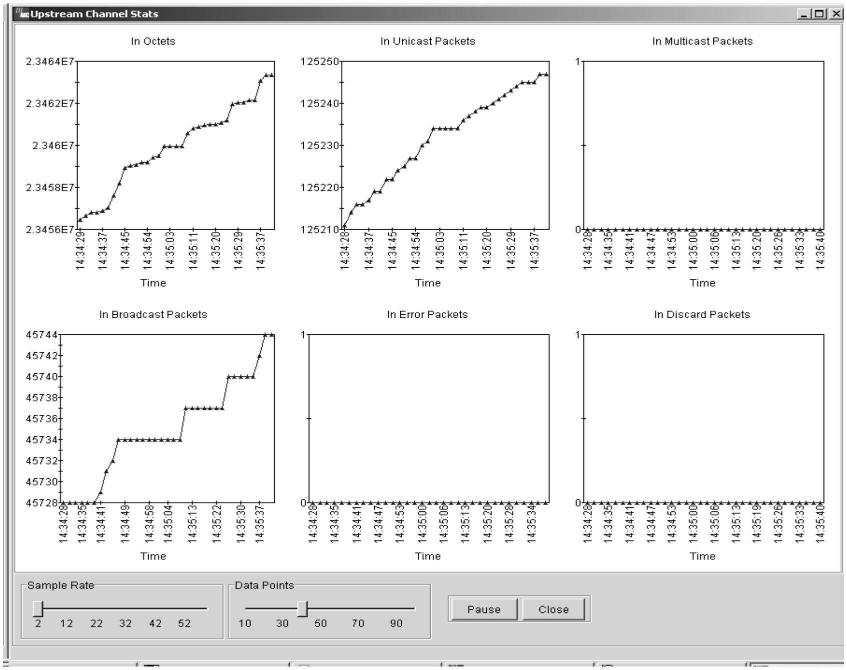
Contents of 'CMTS Interfaces'

Module

Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

Out Discard Packets: 0

Figure 3-26 Real-time Plot of All Parameters



4 MANAGING USER ACCOUNTS

This chapter provides information and procedures on how to manage user accounts, and includes:

- About User Manager
- Accessing User Manager
- Adding User Accounts
- Modifying User Accounts
- Deleting User Accounts

About User Manager

User Manager is an administrative tool to manage Cuda network security, by providing a mechanism to create and manage user accounts. Within User Manager you create a user account, and user profile called an *Access Profile*. The Access Profile contains the user permission to functional areas, and user rights to system configuration functions, called *Access Privileges*.

The Access Profile may include one or a combination of these functional areas:

- **Administrator** — Functions associated with managing user accounts, all network configuration functions, all provisioning functions, and chassis configuration.
- **HFC —** Functions associated with CMTS configuration for DOCSIS or EuroDOCSIS-related parameters, such as configuring downstream and upstream channels and modulation profiles.
- **Provisioning —** Functions associated with provisioning-related tasks, such as configuring DHCP servers, and provisioning cable modems, using the FastFlow Broadband Provisioning Manager.
- **Router** — Functions associated with network router-related tasks, such as configuring IP, RIP and OSPF interfaces.

This table describes the above-named functional areas and the functional associations to the configuration modes:

Configuration Mode:	Functional Area
Cuda Chassis Manager	Administrator, HFC, Router
Fault Management	HFC, Router
Configuration	
IP	Router
Card Summary	HFC, Router
CMTS	HFC
10/100	Router
Gigabit	Router
POS	Router
Chassis Configuration	Administrator

FastFLow BPM 1	Provisioning
Security Management	Administrator

Default Account Information

The Cuda 12000 ships with default user “root,” plus four default Access Profiles, which are:

- **AUDITORPROFILE** — Grants the user with *readonly* rights. The user is granted access to view the HFC, Provisioning and Router functional areas.
- **NOACCESSPROFILE** — Sets a *noaccess* right. The user is restricted from the Administrator, HFC, Provisioning and Router functional areas.
- **OPERATORPROFILE** — Provides the user with *read/write* rights. The user is granted access to view and perform configuration functions in the HFC, Provisioning and Routing functional areas.
- **ROOTPROFILE** — Provides the user with *read/write* rights within the whole the Cuda system. The user is granted full access to the Administrator, HFC, Provisioning and Router functional areas.

You may use the default access profiles to manage user accounts, or you may create new profiles for your particular network environment. To create a new profile refer to section “Creating Profiles”, on page 97.

Accessing User Manager

Following are tips you should know about User Manager:

- You must have ROOTPROFILE privileges—as defined above—to manage user accounts.
- ROOTPROFILE and all default profiles cannot be modified or deleted.

Before You Begin

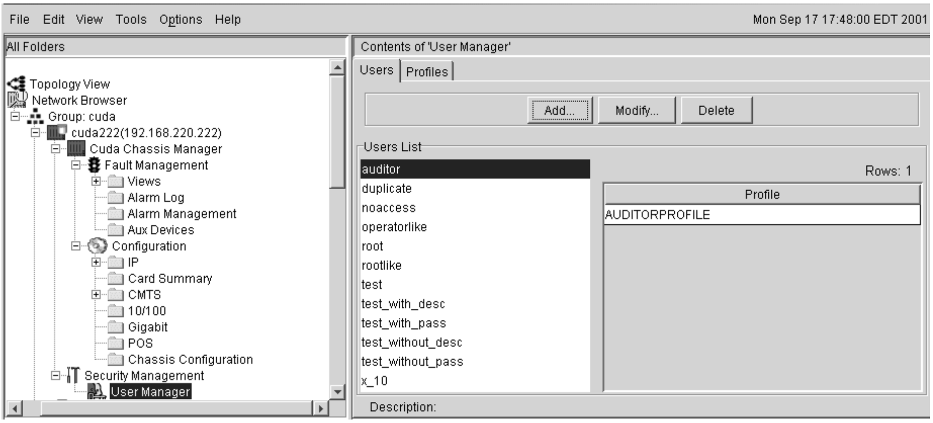
Before you begin to access User Manager, follow this procedure:

1. Navigate to **Network Browser**> **Security Management**> **User Manager**.
2. Click on the **Profiles** tab, or the **Users** tab.

What You See

This figure shows an example of the contents of the **User Manager** window when you fist access it in a session.

Figure 4-1 User Manager Window.



auditor
duplicate
noaccess
operatorlike
root
rootlike
test
test_with_desc
test_with_pass
test_without_desc
test_without_pass
x_10

Profile
AUDITORPROFILE

Creating Profiles

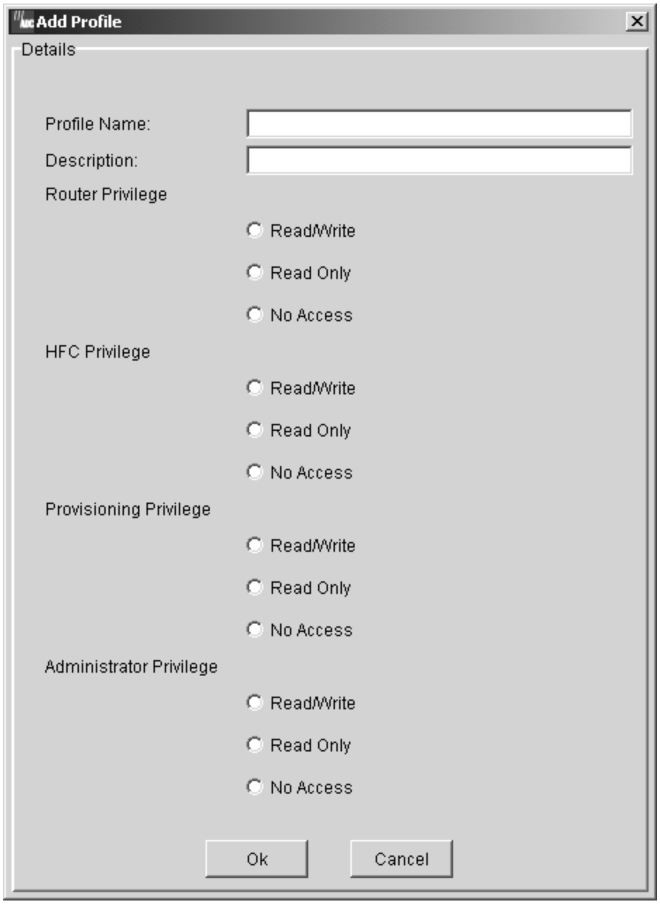
Creating a profile involves assigning a new profile name, granting permissions to functional areas, and assigning functional rights. To create a profile, follow this procedure:

1. From the **Profiles** window, click **Add**. The **Add Profile** window appears.
2. Enter values for the parameters. Refer to .
3. Click **Ok** to add the profile to the system, or click **Cancel** to close the **Add Profile** window without adding the profile to the system.

What You See

This figure shows an example of the **Add Profile** window.

Figure 4-2 Add Profile window



Parameter Descriptions

The following table provides a description of the **Add Profile** window parameters.

Table 4-1 Add Profile Window Parameters

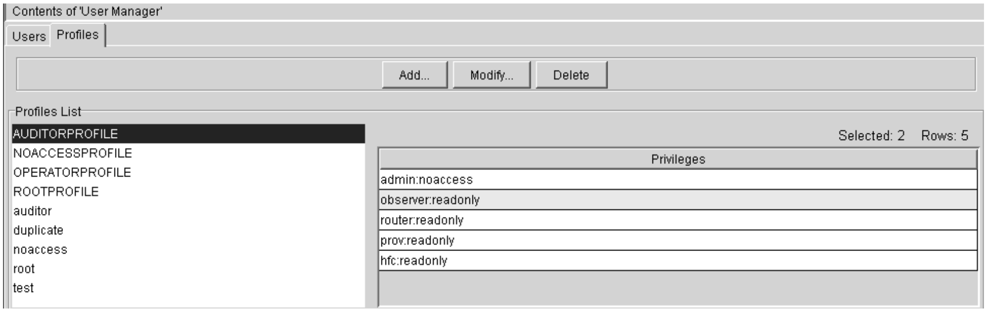
Parameter	Description
Profile Name	Identifies the name for the new profile.
Description	Provides a description of the access privileges for the new profile.
Router Privilege ■ Read/Write ■ Read Only ■ No Access	Grants privileges for router related tasks, such as configuring IP, RIP, and OSPF interfaces.
HFC Privilege ■ Read/Write ■ Read Only ■ No Access	Grants privileges for DOCSIS or EuroDOCSIS associated configurations, such as configuring downstream and upstream channels and modulation profiles.
Provisioning Privilege ■ Read/Write ■ Read Only ■ No Access	Grants privileges for provisioning related tasks, such as configuring DHCP servers, and provisioning cable modems.
Administrator Privilege ■ Read/Write ■ Read Only ■ No Access	Grants privileges for functions related to managing user accounts, such as network configuration functions, provisioning functions, and chassis configuration.

As you grant permissions to functional areas, you assign access rights, called *Access Privileges*, for those functions. The Cuda 12000 supports the following Access Privileges:

- **noaccess —** Prevents the user from viewing or configuring functional areas.
- **readonly** — Allows the user to view system configuration and provisioning. The user is not granted rights to configure the system and manage and view user accounts.
- **read/write —** Provides the user with full system configuration and provisioning rights. The user is not granted rights to manage user accounts.

Figure 4-3. below, displays the privileges for the AUDITORPROFILE.

Figure 4-3 Profiles List Window



AUDITORPROFILE
NOACCESSPROFILE
OPERATORPROFILE
ROOTPROFILE
auditor
duplicate
noaccess
root
test

Selected: 2 Rows: 5

Privileges
admin:noaccess
observer:readonly
router:readonly
prov:readonly
hfc:readonly

***NOTE**: A privilege titled "observer" is listed. Observer provides very limited access to functional areas. The observer privilege may only be configured within the Cuda 12000 base system component. For detail information, refer to the "Cuda 12000 IP Access Switch CLI-based Administration Guide" or "CLI Reference Guide."*

Adding User Accounts

Adding a User account involves entering a username and password, and assigning access profiles, which contain the permissions and rights to system functions. *You must have ROOTPROFILE access to add user accounts*.

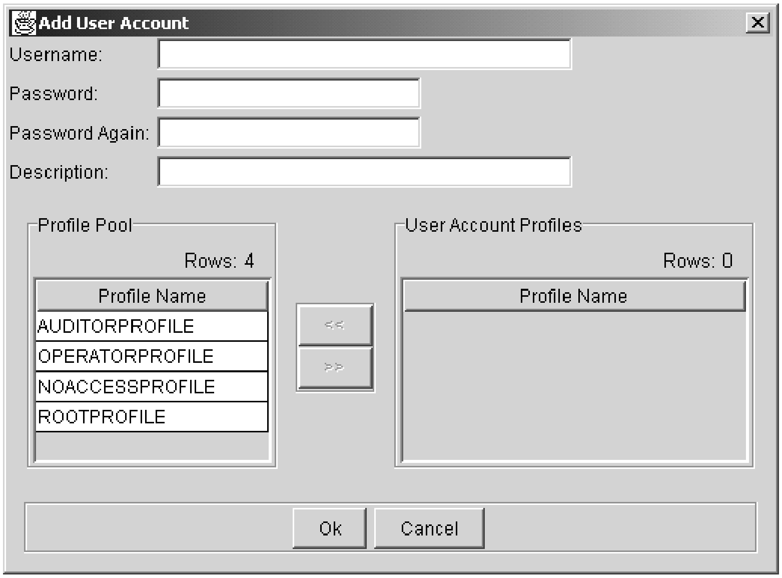
To add a user account, follow this procedure:

1. From the **Users** window, click **Add**. The Add User Account window appears.
2. Enter values for the parameters. Refer to .

3. Click **Ok** to add the user account, or select **Cancel** to close the Add User Account window without adding the user account to the system.

What You See

Figure 4-4 Add User Account Window



Profile Name
AUDITORPROFILE
OPERATORPROFILE
NOACCESSPROFILE
ROOTPROFILE

Profile Name

Parameter Descriptions

This table provides a description of the Add User Account window parameters.

Table 4-2 Add User Account Window Parameters

Parameter	Description
Username	Name of the user account that you want to add. This field is case sensitive.
Password	Password for the account. This field is case sensitive.
Password Again	Confirm the password that you specified for the account.

Parameter	Description
Description	The administrator defines a description for this user.
Profile Name	Assign a profile to the user. From the Profile Pool list, select the Profile Name for the user. Using the ">>" toggle button, move the selected Profile Name to the User Account Profiles column. You may assign more than one access profile to a user account. For a description of the Profile Names, refer to the section "Default Account Information"on page 95. **NOTE**: When you add more than one access profile, the profile with more rights takes precedence.

Modifying User Accounts

Modifying a user account allows you to do the following. You must have ROOTPROFILE access to modify user accounts:

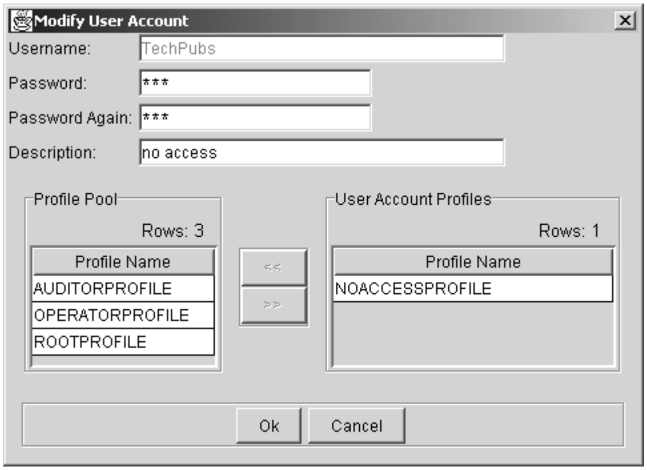
- Change a user password
- Change a user description
- Change a user profile

Follow this procedure to modify an existing user account:

1. From the Users window, select the user account you wish to modify and click **Modify**. The Modify User Account window appears.
2. Update the account information. Toggle between the ""<<"and ">>" buttons to add or remove a profile.
3. Click **Ok** to commit the changes, or click **Cancel** to close the window without making changes to the existing account.

What You See

Figure 4-5 Modify User Account window.



Modify User Account

Username: TechPubs

Password: ***

Password Again: ***

Description: no access

Profile Pool

Rows: 3

Profile Name
AUDITORPROFILE
OPERATORPROFILE
ROOTPROFILE

User Account Profiles

Rows: 1

Profile Name
NOACCESSPROFILE

Deleting User Accounts

Deleting a user account locks that user out of the system. You must have ROOTPROFILE access to remove user accounts.

Follow this procedure to delete a user account from the system:

1. From the Users window, select the user account you wish to delete, and click on **Delete**. The Delete User Account window appears.
2. Click **Yes** to delete the account, or click **No** to cancel the deletion.

II

CHASSIS ADMINISTRATION

5 CHASSIS MANAGEMENT

This chapter describes chassis management and chassis configuration functions, and includes the following sections:

- Understanding Chassis Identification
- Understanding Management Module Redundancy
- Configuring a Chassis
- Configuring Traffic Relay

***NOTE**: You must have access privileges to the Administrator functional area to perform chassis configuration. For more information about access privileges, refer to chapter 3 Managing User Accounts.*

Understanding Chassis Identification

The Cuda 12000 supports the following chassis environment:

- a multiple-chassis environment, in which multiple chassis are connected through a network environment but do not form a single router.

Each Cuda 12000 should be configured with a *unique* chassis identification (ID) number. The chassis ID serves as a router management tool.

Understanding Management Module Redundancy

Each chassis is equipped with at least one management module, which controls the chassis. For management module redundancy, the Cuda 12000 supports installation of two management modules. When two management modules are installed, one acts as the *primary* management module and the other acts as the *secondary* management module.

When a Cuda 12000 that is configured with two management modules reboots, the Cuda 12000 randomly determines which module acts as the primary and which module acts as the secondary. The STATUS DISPLAY LED on the management module indicates whether the management module is a primary or secondary (for example, the LED on a primary management module displays "PRIMARY").

The primary management module is the active management module on the Cuda 12000. When you use CudaView to manage the Cuda 12000, you are interacting with the primary management module.

The secondary management module has two responsibilities:

- Monitor the state of the primary management module
- Keep its mirrored disk sectors synchronized with the primary management module

A secondary management module can take over the primary role in two ways:

- Automatically, when the secondary management module detects that the primary management module is not functioning properly.
- Manually, through the Chassis Designation tab. In this case, you use the command to force the current primary management module into the secondary role, which in turn forces the current secondary management module into the primary role.

When the secondary management module takes over the primary role, the secondary:

- Activates its copy of the Cuda 12000 software
- Establishes connections with all other cards in the chassis

When the secondary management module activates its copy of the Cuda 12000 software and establishes connections to cards, the secondary management module also starts services, including disk-mirroring and LDAP. Through disk mirroring, the software on the two management modules share data.

When a switch to a secondary management module occurs:

- Services are unavailable for a brief period of time
- Network management access is prevented for a brief period of time.

The Cuda's data-forwarding operation is not disrupted while a switchover to a backup occurs.

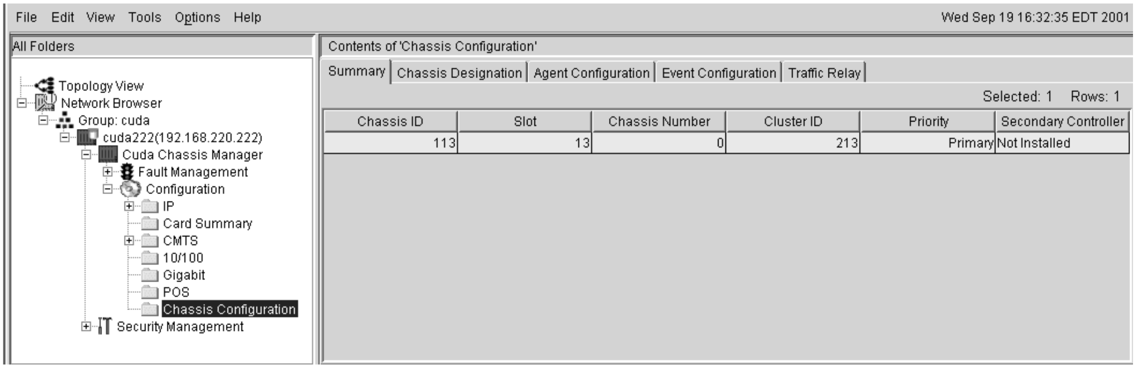
Configuring a Chassis

Configuring a chassis consists of these functions:

- Assigning or changing chassis and cluster IDs.
- Defining in which slot the Primary module resides.
- Defining if the Primary module is managing a cluster or independent chassis environment.

Figure 5-1 is an example of the **Summary** window. This window displays chassis identification information for only the primary management module. *(Configuration information for the Agent Configuration tab is explained in Chapter 7, "Simple Network Management Protocol (SNMP)". Configuration information for the Event Configuration tab is explained in Chapter 8, "Managing System Events".)*

Figure 5-1 Chassis Configuration Summary Window



Selected: 1 Rows: 1

Chassis ID	Slot	Chassis Number	Cluster ID	Priority	Secondary Controller
113	13	0	213	Primary	Not Installed

Table 5-1 Parameter Descriptions of Summary Window

Parameter	Description
Chassis ID	Unique identification number you assign to a Cuda 12000 chassis in the network. The Cuda uses a multi-range numbering system. Acceptable chassis ID values are 1 to 128. The Cuda defaults with chassis number 255. We recommend that you do not change the chassis ID. This may cause the Cuda 12000 to lose the configuration that is saved on the provisioning database, as well as other persisted files.
Slot	Indicates the slot number in which the Primary management module is located. The Primary management module resides in slot 13 or 14.
Chassis Number	Serial number assigned to the chassis during manufacturing.
Cluster ID	User-defined. Identifies the cluster in which the Cuda 12000 is a member. Acceptable Cluster ID values are 0 to 2147483647.
Priority	Indicates if the module in the specified slot is designated as the primary or secondary module. The options are: ■ Primary: Indicates the module in the specified slot is the primary management module. ■ Active Standby: Indicates that a second management module is installed but is not activated. ■ Not Installed: Indicates that only one management module is installed.
Secondary Controller	Indicates if the secondary module is active or installed. The options are: ■ Primary: Indicates the secondary module in the specified slot is the primary management module. ■ Active Standby: Indicates that the secondary management module is installed but is not activated. ■ Not Installed: Indicates that only one management module is installed.

Perform the following tasks to configure a chassis:

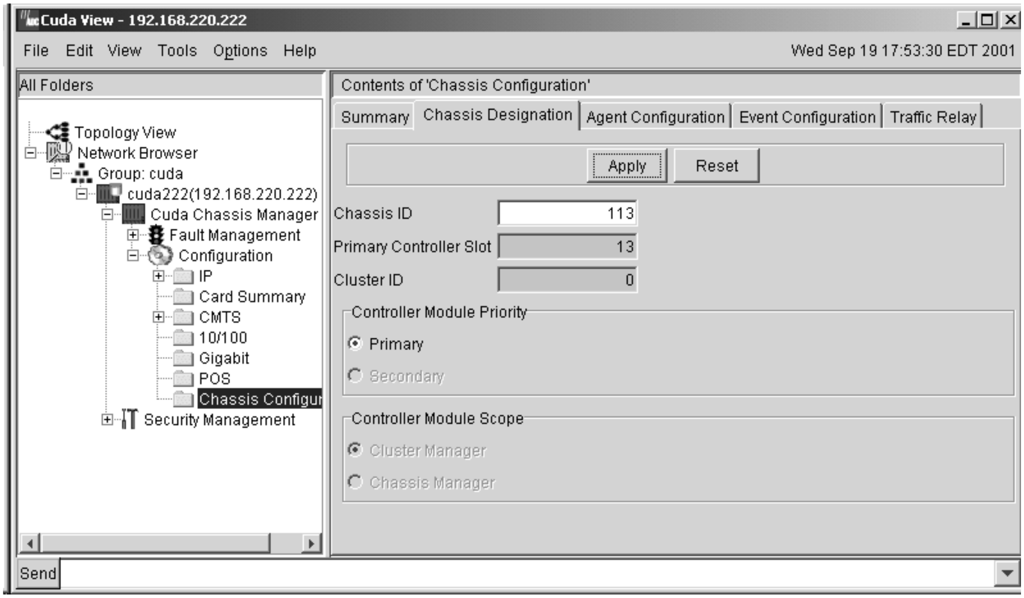
Navigation Path

GroupName>ChassisName>**Cuda Chassis Manager>Configuration**

Procedure

1. Click the **Summary** tab.
2. In the **Summary** window, select the row that includes the chassis or cluster ID that you want to modify.
3. Click the **Chassis Designation** tab.
4. Enter values for the parameters.
5. Click **Apply** to commit the information or click **Reset** to return to the previous values.
6. If you changed the Chassis ID**,** then you must restart all management and application modules to reload your latest services. To restart the chassis, use the normal Linux reboot mechanism.What You See

Figure 5-2 Chassis Designation window



Chassis ID: 113

Primary Controller Slot: 13

Cluster ID: 0

Controller Module Priority

● Primary

○ Secondary

Controller Module Scope

● Cluster Manager

○ Chassis Manager

Parameter Descriptions

This table provides a description of the Chassis Designation window

Table 5-2 .Chassis Designation Window Parameters

Parameter	Description
Chassis ID	Specifies the new chassis ID for this Cuda 12000 in the network. The Cuda 12000 uses a multi-range numbering system. Acceptable chassis ID values are 1 to 128, or 255. The default is one.
Primary Controller Slot	Read-only. This indicates the slot in which the primary management module is installed.
Cluster ID	Specifies the cluster ID to identify the cluster to which the Cuda 12000 belongs. A Cluster ID is also assigned to a chassis in a chassis-independent environment as the chassis currently supports a cluster of 11. Acceptable range is 0 to 2147483647.
Controller Module Priority	Enables you to force the current primary management module into a secondary role; thereby, forcing the current secondary management module into the primary role.

Parameter	Description
Slot 13	Select if the management module is in slot 13 and you want it to be the primary controller. Slot 13 is the default.
Slot 14	Select if the management module is in slot 14 and you want it to be the primary controller.
Controller Module Scope	Indicates whether the primary and secondary management modules are managing a chassis or cluster environments.
Cluster Manager	Select if the management module is controlling a cluster-network environment.
Chassis Manager	Select if the management module is controlling a chassis-independent environment.

Configuring Traffic Relay

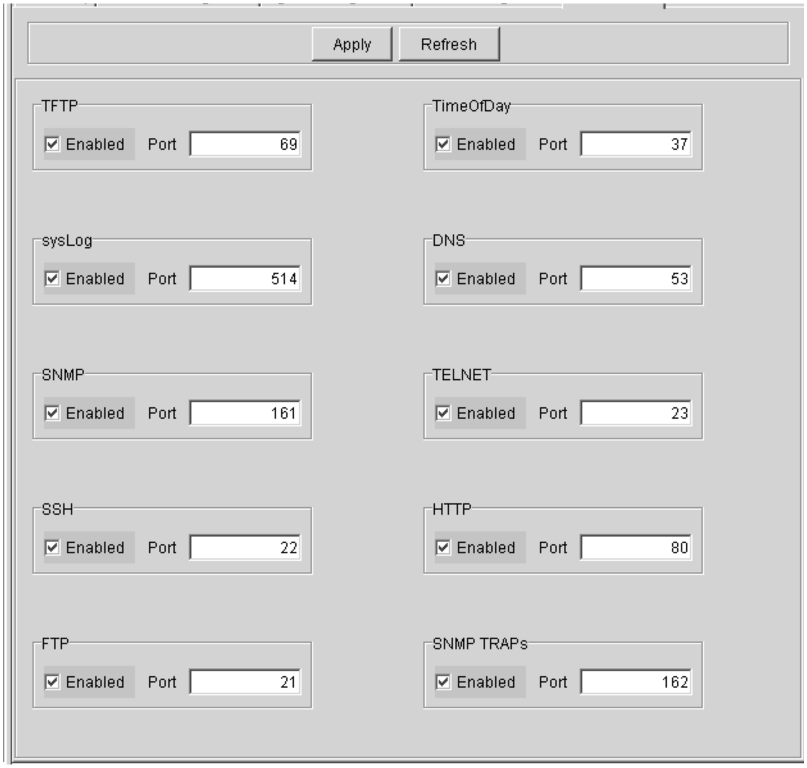
The traffic relay function configures processes, such as the HTTP server, to send and receive TCP or UDP packets using an internal address on the Cuda 12000, for in-band management. For example, you can enable forwarding of Telnet traffic and HTTP traffic using an internal address, thereby allowing you to perform in-band management of the Cuda 12000 using the CLI or CudaView.

To enable or disable traffic relay options, follow these procedures:

1. Navigate to GroupName>ChassisName> **Cuda Chassis Manager** > **Configuration** > **Chassis Configuration**.
2. Click the **Traffic Relay** tab.
3. For each server, select **Enable** option and enter the destination port number to enable the relay of UDP/TCP traffic in the Cuda 12000.
4. To disable the traffic, clear the option.
5. Click **Apply** to commit the information.
6. Click **Refresh** to update the information.

What You See

Figure 5-3 Traffic Relay window.



TFTP
☑ Enabled Port 69

TimeOfDay
☑ Enabled Port 37

sysLog
☑ Enabled Port 514

DNS
☑ Enabled Port 53

SNMP
☑ Enabled Port 161

TELNET
☑ Enabled Port 23

SSH
☑ Enabled Port 22

HTTP
☑ Enabled Port 80

FTP
☑ Enabled Port 21

SNMP TRAPs
☑ Enabled Port 162

NOTE: If you are running a TFTP server on the Cuda 12000 as part of FastFlow BPM provisioning, you must enable traffic relay for the TFTP server in order to download configuration files to cable modems. The TFTP server sends and receives packets using an internal address. Refer to the FastFlow BPM documentation set for more information on the FastFlow BPM.

6 MANAGING MULTIPLE CHASSIS

Multi-chassis support allows the network administrator to manage multiple Cuda chassis while logged into the chassis containing the Java applet (the chassis where you have logged in using a GUI login screen). Communication between this chassis and another chassis within the group is by proxy. The GUI on the chassis directly talks to a Java server that can proxy requests to other Java servers for other chassis in the same group and subnet.

Chassis in the same group and subnet as the GUI chassis are discovered by a location server. You cannot communicate with chassis in a different group or on a different subnet.

By default, the location server is set not to perform discovery and each chassis is enabled for discovery. You can reconfigure these settings with the command line interface (CLI) from your CLI console window (refer to Chapter 3, "CudaView Desktop Tools" for information on the CLI console window). For a description of CLI commands and settings, refer to the *Cuda 12000 IP Access Switch CLI Reference Guide* and *Cuda 12000 IP Access Switch CLI-based Administration Guide*. The CLI console window is available only when you are logged into, and have selected, the GUI client chassis.

Cuda chassis ship with a pre-assigned default group, which is 'Cuda'; no other groups are currently supported. However, you can rename the default group using the CLI in your console window.

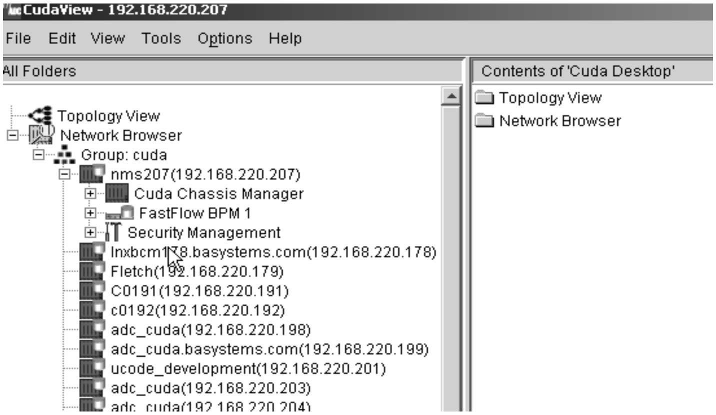
When you browse back and forth between the GUI client chassis and another chassis, only the context is switched. This means that you are not establishing a new session when you select another chassis, nor are you logging out of the GUI client. Instead, you remain logged in and in session with the GUI client chassis.

Accessing a Chassis Other Than the GUI Client

You access other chassis by clicking on the symbol to the left of the desired chassis.

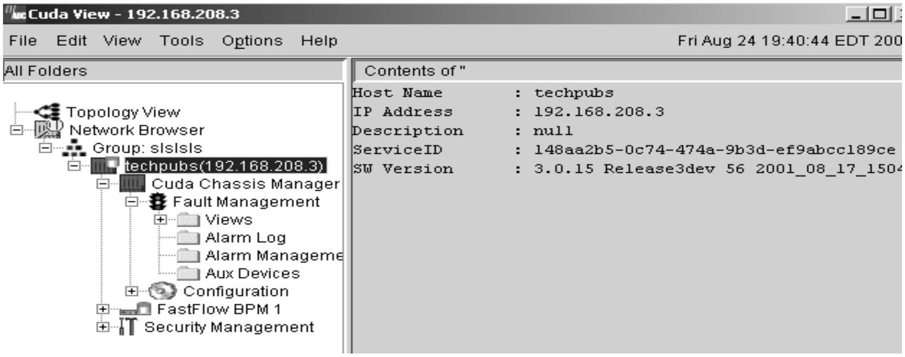
You can view multiple chassis in either panel. When you log in to a GUI client, the initial screen (see Figure 6-1, "Initial Multi-Chassis Display") shows the default group and all chassis in the group that are enabled.

Figure 6-1 Initial Multi-Chassis Display



If chassis are not already displayed, click on the symbol to the left of the group name in order to expand it into its member chassis. Figure 6-2, "Example of a Right Panel Display of Chassis in a Group", illustrates a right-panel display of chassis in a selected group.

Figure 6-2 Example of a Right Panel Display of Chassis in a Group



```
Host Name        : techpubs
IP Address       : 192.168.208.3
Description      : null
ServiceID        : 148aa2b5-0c74-474a-9b3d-ef9abcc189ce
SW Version       : 3.0.15 Release3dev 56 2001_08_17_1504
```

Managing a Chassis Other Than the GUI Client

Selecting a chassis symbol in the left panel by clicking on it performs the following functions:

- Displays chassis node information in the right panel (Figure 6-2).
- Expands the directory structure, in the left panel, associated with the chassis folder (Figure 6-2).
- Checks your initial login against the user profile on the chassis that is not the GUI client chassis and grants access accordingly. You remain logged in to the GUI client chassis.

Requirements for accessing a chassis other than the GUI client:

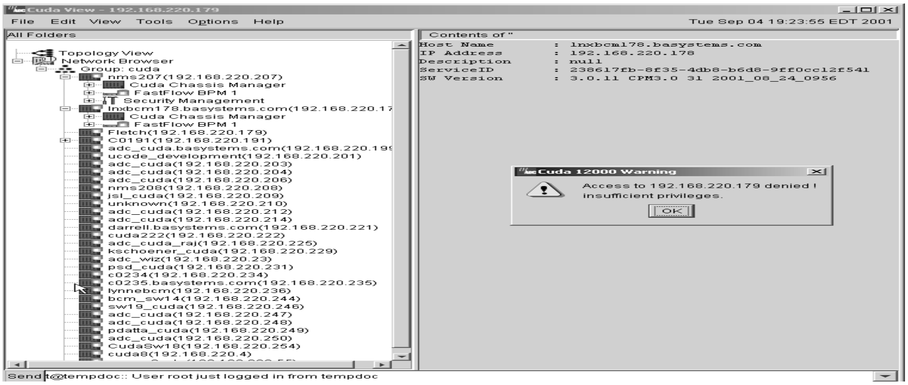
- The GUI login must match to a user account on the chassis to be selected, or else you receive a "Denied Access" message (Figure 6-3, “Denied Access Message”).
- The version number of the selected chassis must be compatible with the version number of the GUI client as follows: numbers to the left of the decimal point must match. For example, versions 3.15 and 4.0 are not compatible, but versions 3.25 and 3.35 are. If versions are not compatible, no further information and no sub-hierarchy appears for the selected chassis.

Requirements for managing a chassis other than the GUI client:

- Access to the chassis’ management functions is determined by the user profile residing on the selected chassis and not by your user profile on the GUI client.

Note: You must select the GUI client chassis in order to access CLI Console and Trace Log in the Tools Menu. In a multi chassis environment you do not have access to Trace Route or BAS Ping unless you select a chassis other than the GUI client..

Figure 6-3 Denied Access Message



```
Topology View
Network Browser
  Group: cuda
    nms207(192.168.220.207)
      Cuda Chassis Manager
      FastFlow BPM 1
      Security Management
    lnxbcm178.basystems.com(192.168.220.17
      Cuda Chassis Manager
      FastFlow BPM 1
    Fletch(192.168.220.179)
    C0191(192.168.220.191)
    adc_cuda.basystems.com(192.168.220.19
    ucode_development(192.168.220.201)
    adc_cuda(192.168.220.203)
    adc_cuda(192.168.220.204)
    adc_cuda(192.168.220.206)
    nms208(192.168.220.208)
    jsl_cuda(192.168.220.209)
    unknown(192.168.220.210)
    adc_cuda(192.168.220.212)
    adc_cuda(192.168.220.214)
    darrell.basystems.com(192.168.220.221)
    cuda222(192.168.220.222)
    adc_cuda_raj(192.168.220.225)
    kschoener_cuda(192.168.220.229)
    adc_wiz(192.168.220.23)
    psd_cuda(192.168.220.231)
    c0234(192.168.220.234)
    c0235.basystems.com(192.168.220.235)
    lynnebcm(192.168.220.236)
    bcm_sw14(192.168.220.244)
    sw19_cuda(192.168.220.246)
    adc_cuda(192.168.220.247)
    adc_cuda(192.168.220.248)
    pdatta_cuda(192.168.220.249)
    adc_cuda(192.168.220.250)
    CudaSw18(192.168.220.254)
    cuda8(192.168.220.4)
```

```
Host Name        :  lnxbcml78.basystems.com
IP Address       :  192.168.220.178
Description      :  null
ServiceID        :  238617fb-8f35-4db8-b6d8-9ff0cc12f541
SW Version       :  3.0.11 CPM3.0 31 2001_08_24_0956
```

Cuda 12000 Warning

Access to 192.168.220.179 denied !
insufficient privileges.

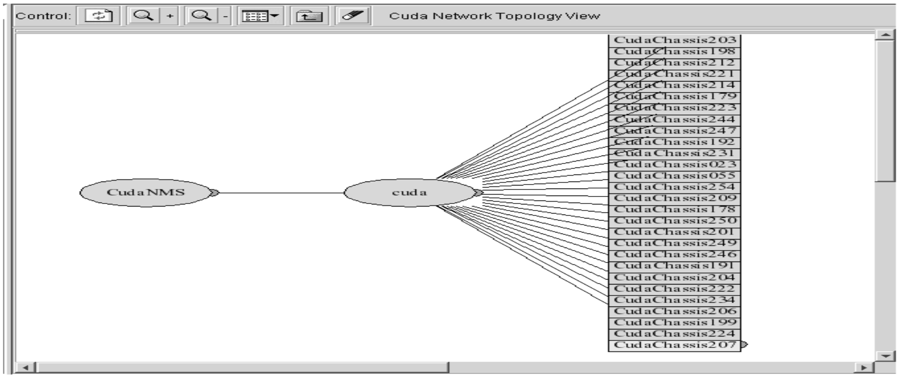
OK

t@tempdoc:: User root just logged in from tempdoc

Topology View of the Multi-chassis Network

You can use the Topology View for a network view of the default group and its chassis.

Figure 6-4 Viewing Default Group and Member Chassis Using Topology View



Refer to Chapter 2, “Getting Started”for more information on using the Topology view for a particular chassis.

7 SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

Simple Network Management Protocol (SNMP) governs the network management and monitoring of network devices and their functions. In addition, SNMP provides secure access to these devices by strategies that can consist of authorizing, authenticating and encrypting SNMP packeting over a network.

SNMPv3 includes the SNMPv3 entity. An SNMPv3 entity consists of an SNMP engine and SNMPv application. The SNMP engine has the functionality of both the SNMP agent and SNMP manager.

This chapter describes SNMP configuration on the Cuda 12000 and includes the following sections:

- Configuring SNMP Agent Parameters
- Configuring SNMPv3 Contexts
- Configuring SNMPv3 Users
- Configuring SNMP Groups
- Configuring SNMP Access Views
- Configuring SNMP Communities
- Configuring SNMP Notifications
- Selecting SNMP Notification Types

SNMP Security

SNMP controls access according to three security models: SNMPv1, SNMPv2c, and SNMPv3.

A security level is the permitted level of security within a security model. SNMPv1, SNMPv2c, and SNMPv3 differ in the level of security they provide. SNMPv1 and SNMPv2c perform no authentication that, for example, safeguards against spoofing. For these models, Cuda 12000 supports no authentication, but supports authentication of identity and privacy through encryption for SNMPv3.

The bases for access control for each of the security versions is shown in ().

Table 7-1 Access Control for Security Versions

SNMPv1	SNMPv2c	SNMPv3
communities	communities	users
		contexts
groups	groups	groups
MIB views	MIB views	MIB views

Configuring SNMP Agent Parameters

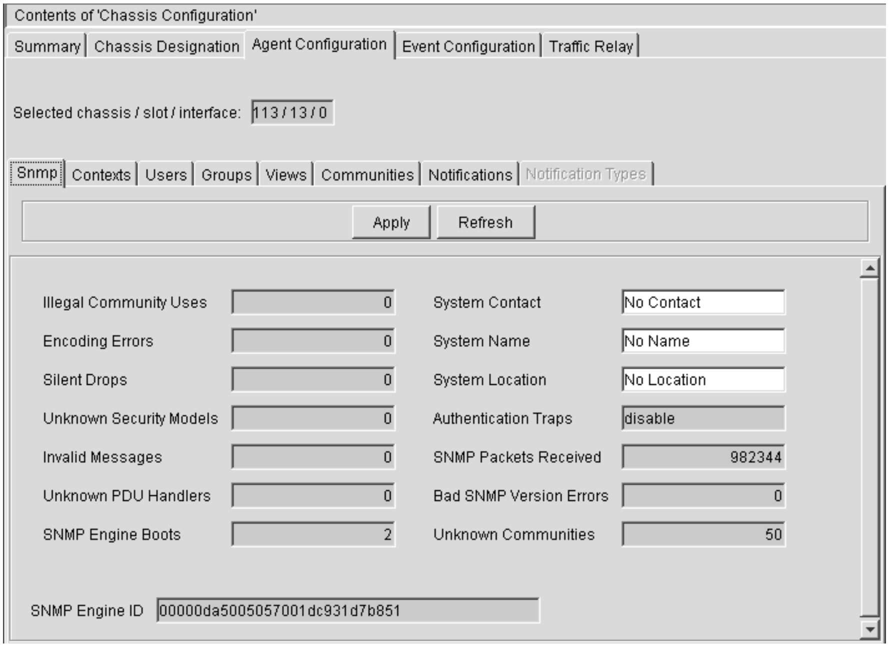
Follow this procedure to configure SNMP agent parameters and view statistics:

Procedure

1. Navigate to **Network Browser**> GroupName>ChassisName> **Cuda Chassis Manager** > **Configuration** > **Chassis Configuration**
2. Click the **Summary** tab.
3. In the Summary window, select the chassis, slot, and interface that you wish to configure.
4. Click the **Agent Configuration** tab.
5. In the **Agent Configuration** window, click the **Snmp** tab. The Agent Configuration window appears.
6. Enter values for the parameters. Refer to Table 7-2.
7. Click **Apply** to commit the changes.
8. Click **Refresh** to update the information.

What You See

Figure 7-1 Snmp window



Selected chassis / slot / interface: 113 / 13 / 0

Illegal Community Uses 0

Encoding Errors 0

Silent Drops 0

Unknown Security Models 0

Invalid Messages 0

Unknown PDU Handlers 0

SNMP Engine Boots 2

System Contact No Contact

System Name No Name

System Location No Location

Authentication Traps disable

SNMP Packets Received 982344

Bad SNMP Version Errors 0

Unknown Communities 50

SNMP Engine ID 00000da5005057001dc931d7b851

Parameter Descriptions

This table provides a description of the Snmp window parameters:

Table 7-2 SNMP Agent Parameters

Parameter	Description
Illegal Community Uses	Read only. Total number of SNMP messages that the SNMP entity receives that represent an SNMP operation that is now allowed by the SNMP community named in the message.
Encoding Errors	Read only. Total number of ASN.1 or BER errors that the SNMP entity encounters when decoding SNMP messages.
Silent Drops	Read only. Total number of GetRequest-PDUs, GetNextRequest-PDUs, GetBulkRequest-PDUs, SetRequest-PDUs, and InformRequest-PDU packets that the SNMP entity receives and drops.

Parameter	Description
Unknown Security Models	Read only. Total number of packets that the SNMP engine receives and drops because the security model was not known or supported by the SNMP engine.
Invalid Messages	Read only. Total number of packets that the SNMP engine receives and drops because there were invalid or inconsistent components in the SNMP message.
Unknown PDU Handlers	Read only. Total number of packets that the SNMP engine receives and drops because the PDU contained in the packets could not be passed to an application responsible for the PDU type.
SNMP Engine Boots	Read only. Number of times the SNMP engine initializes since the last SNMP Engine ID configuration.
System Contact	The name of a system contact.
System Name	The name of the system.
System Location	The location of the system.
Authentication Traps	Read only. Indicates whether the SNMP entity is able to generate failure traps.
SNMP Packets Received	Read only. Total number of messages that the transport service delivers to the SNMP entity.
Bad SNMP Version Errors	Read only. Total number of SNMP messages that the SNMP entity receives using an unsupported version of SNMP.
Unknown Communities	Read only. Total number of SNMP messages that the SNMP entity receives using an SNMP community name not known to the entity.
SNMP Engine ID	Read only. The SNMP engine’s unique identifier. This is a 14-byte octet string.

Configuring SNMPv3 Contexts

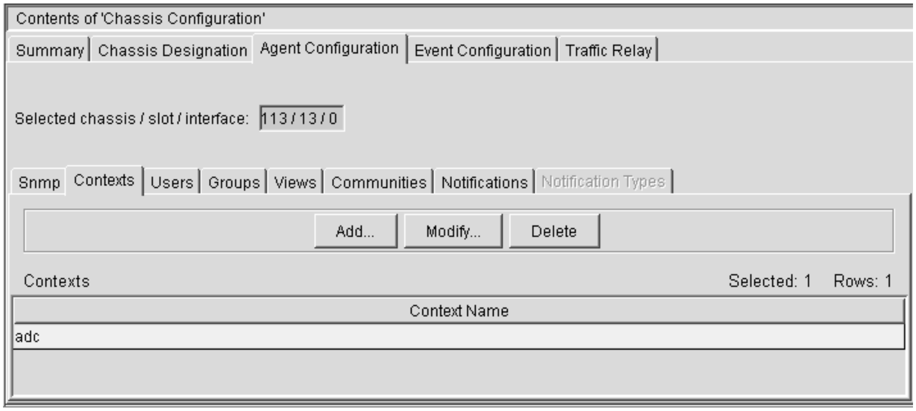
A context in SNMPv3 is a collection of management information accessible by an SNMP entity. You can view, add, modify, or delete SNMP contexts.

Follow this procedure:

1. Navigate to **Network Browser>**GroupName>ChassisName>**Cuda Chassis Manager**>**Configuration** > **Chassis Configuration.**
2. In the Summary window, select the chassis, slot, and interface that you wish to configure.
3. Click the **Agent Configuration** tab. The Agent Configuration window appears.
4. Click the **Contexts** tab. The Contexts window appears.

What You See

Figure 7-2 Contexts window.



Selected chassis / slot / interface: 113 / 13 / 0

Contexts Selected: 1 Rows: 1

Context Name
adc

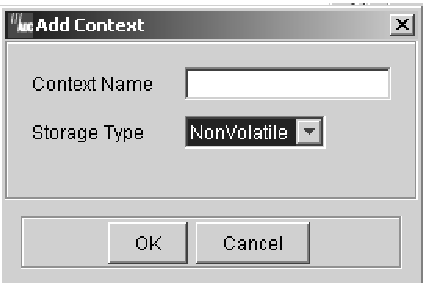
Adding Contexts

Follow this procedure to add an SNMP context:

1. In the Contexts window, click **Add**. The Add Context window appears.
2. Enter values for the parameters. Refer to Table 7-3.
3. Click **Ok** to commit the changes or click **Cancel** to exit without saving.

What You See

Figure 7-3 Add Context window.



Parameter Descriptions

This table provides a description of the Add Context window

Table 7-3 SNMPv3 Add Context Window Parameters.

Parameter	Description
Context Name	Name that identifies a context. A name that is of zero length indicates a default context.
Storage Type	Storage type for this context.
Volatile	Entry is stored in volatile memory. The information is lost during a system reboot.
Non-volatile	Entry is stored in non-volatile memory. The information is not lost during a system reboot.
Permanent	Entry is stored in non-volatile memory. You cannot delete the information but you can make modifications.
Read-only	Entry is stored in non-volatile memory. You cannot delete or modify the information.

Modifying SNMPv3 Contexts

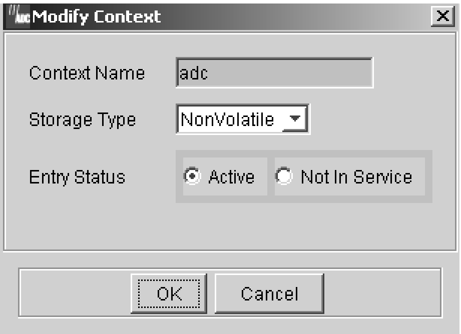
Follow this procedure to modify an SNMPv3 context:

1. In the Contexts window, click **Modify**. The Modify Context window appears.
2. Modify the required options. Refer to Table 7-4.

3. Click **Ok** to commit the changes or click **Cancel** to return to the Context window without saving.

What You See

Figure 7-4 Modify Context window.



Context Name: adc

Storage Type: NonVolatile

Entry Status: ● Active ○ Not In Service

Parameter Descriptions

This table provides a description of the Modify Context window

Table 7-4 SNMPv3 Modify Context Window Parameters.

Parameter	Description
Context Name	Read only. Name that identifies a context.
Storage Type	Storage type for this context.
Volatile	Entry is stored in volatile memory. The information is lost during a system reboot.
Non-volatile	Entry is stored in non-volatile memory. The information is not lost during a system reboot.
Permanent	Entry is stored in non-volatile memory. You cannot delete the information but you can make modifications.
Read-only	Entry is stored in non-volatile memory. You cannot delete or modify the information.
Entry Status	Allows you to enable or disable an entry.
Active	Actives an entry.
Not In Service	Allows you to temporarily disable the entry.

Deleting SNMPv3 Contexts

Follow this procedure to delete an SNMPv3 context:

1. In the Contexts window, select the context you wish to delete.
2. Click **Delete**. A confirmation window appears.
3. Click **Yes** to continue or click **No** to cancel the deletion.

Configuring SNMPv3 Users

The SNMPv3 user is anyone who requires management operations to be authorized by a particular SNMP entity. SNMP entities must have knowledge of a user and the user’s attributes.

You can view, add, modify, or delete users.

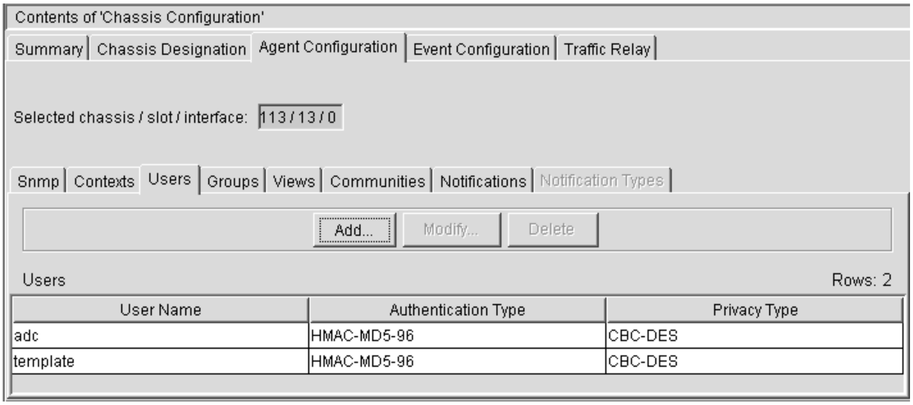
Before You Begin

Before you configure users for SNMPv3, follow this procedure:

1. Navigate to **Network Browser**>GroupName>ChassisName> **Cuda Chassis Manager**>**Configuration**>**Chassis Configuration**.
2. In the Summary window, select the chassis, slot, and interface that you wish to configure.
3. Click the **Agent Configuration** tab. The Agent Configuration window appears.
4. Click the **Users** tab. The Users window appears. Refer to Figure 7-5.

What You See

Figure 7-5 Users window



Selected chassis / slot / interface: 113 / 13 / 0

Users Rows: 2

User Name	Authentication Type	Privacy Type
adc	HMAC-MD5-96	CBC-DES
template	HMAC-MD5-96	CBC-DES

Parameter Descriptions

This table provides a description of the Users window parameters

Table 7-5 SNMPv3 Users Window Parameters.

Parameter	**Description**
User Name	Name of the user.
Authentication Type	Type of authentication that verifies from whom the message is from and whether the messages is altered. The options are: HMAC-MD5-96, HMAC-SHA-96, or none.
Privacy Type	Encrypts user data for privacy. The options are: Cypher Block Chaining using the Data Encryption Standard (CBC-DES) or none.

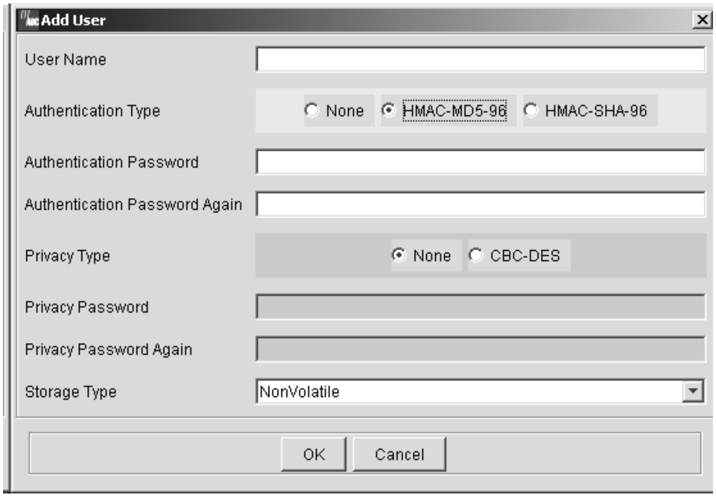
Adding SNMPv3 Users

Follow this procedure to add a user:

1. In the Users window, click **Add**. The Add User window appears.
2. Enter values for the parameters. Refer to Table 7-6.
3. Click **Ok** to commit changes or **Cancel** to exit window without saving.

What You See

Figure 7-6 Add SNMPv3 User window.



User Name

Authentication Type ○ None ● HMAC-MD5-96 ○ HMAC-SHA-96

Authentication Password

Authentication Password Again

Privacy Type ● None ○ CBC-DES

Privacy Password

Privacy Password Again

Storage Type NonVolatile

Parameter Descriptions

This table provides a description of the Add User window parameters

Table 7-6 SNMP Add User Window Parameters:

Parameter	Description
User Name	Name of the user. Range is 1 to 32 characters.
Authentication Type	Enables you to select the authentication type used to authenticate the user.
Authentication Password	Password key for authentication. If the authentication type is HMAC-MD5-95 or HMAC-SHA-96, you must enter a password for authentication. The password must be an ASCII Hex string with a maximum size of 40 characters (20 bytes). Password is write-only for security purposes. You must enter the password each time you make a modification.
Privacy Type	Encrypts data for privacy according to the DES (Data Encryption Standard) algorithm.
Privacy Password	Password for the privacy type. The password must be an ASCII Hex string with a maximum size of 64 character (32 bytes).

Parameter	Description
Storage Type	Storage type for this entry.
Volatile	Entry is stored in volatile memory. The information is lost during a system reboot.
Non-volatile	Entry is stored in non-volatile memory. The information is not lost during a system reboot.
Permanent	Entry is stored in non-volatile memory. You cannot delete the information but you can make modifications.
Read-only	Entry is stored in non-volatile memory. You cannot delete or modify the information.

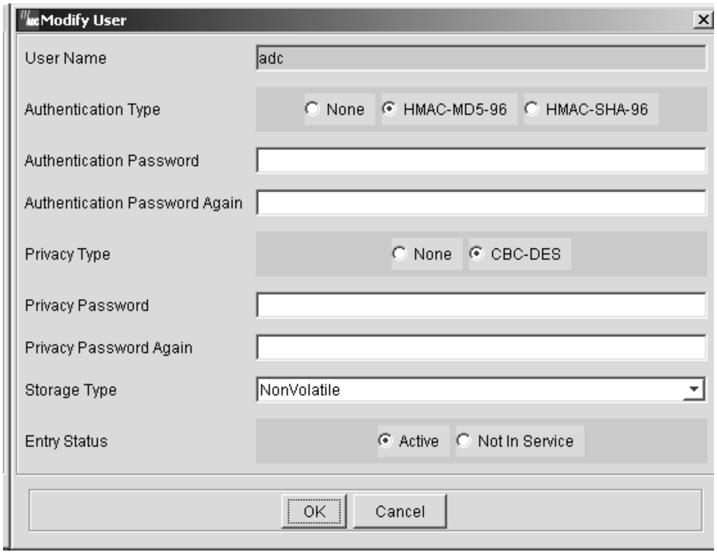
Modifying SNMPv3 Users

Follow this procedure to modify a user:

1. In the User window, select the user you wish to modify and click **Modify**. The Modify User window appears.
2. Update the necessary information. Refer to Figure 7-7.
3. Click **Apply** to commit the changes or click **Cancel** to exit without saving.

What You See

Figure 7-7 This figure shows an example of the Modify User window.



Modify User

User Name: adc

Authentication Type: ○ None ● HMAC-MD5-96 ○ HMAC-SHA-96

Authentication Password:

Authentication Password Again:

Privacy Type: ○ None ● CBC-DES

Privacy Password:

Privacy Password Again:

Storage Type: NonVolatile

Entry Status: ● Active ○ Not In Service

Parameter Descriptions

This table provides a description of the Modify User window parameters

Table 7-7 SNMPv3 Modify User Window Parameters:

Parameter	Description
User Name	Name of the user. Range is 1 to 32 characters.
Authentication Type	Enables you to select the authentication type used to authenticate the user.
Authentication Password	Password key for authentication. If the authentication type is HMAC-MD5-95 or HMAC-SHA-96, you must enter a password for authentication. The password must be an ASCII Hex string with a maximum size of 40 characters (20 bytes).
	Password is write-only for security purposes. You must enter the password each time you make a modification.
Privacy Type	Encrypts data for privacy according to the DES algorithm.
Privacy Password	Password for the privacy type. The password must be an ASCII Hex string with a maximum size of 64 character (32 bytes).
Storage Type	Storage type for this entry.
Volatile	Entry is stored in volatile memory. The information is lost during a system reboot.
Non-volatile	Entry is stored in non-volatile memory. The information is not lost during a system reboot.
Permanent	Entry is stored in non-volatile memory. You cannot delete the information but you can make modifications.
Read-only	Entry is stored in non-volatile memory. You cannot delete or modify the information.
Entry Status	Allows you to enable or disable an entry.
Active	Actives an entry.
Not In Service	Allows you to temporarily disable the entry.

Deleting SNMPv3 Users

Follow this procedure to delete a user:

1. In the Users window, select the user you with to delete.
2. Click **Delete**. A confirmation window appears.
3. Click **Yes** to commit the changes or click **No** to cancel the deletion.

Configuring SNMP Groups

The purpose of configuring a group is to differentiate access with respect to specific combinations of context, security model, security level, and view access. You may add, modify, and delete groups.

SNMPv1 and SNMPv2c do not recognize context separately, but do recognize context when you have associated it with a Group, as described in the next procedure.

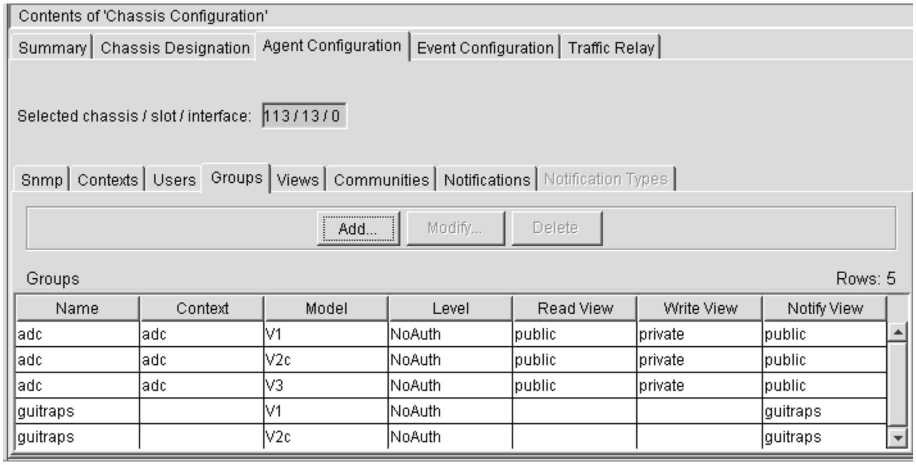
Before You Begin

Before you configure groups, follow this procedure:

1. Navigate to **Network Browser**>GroupName>ChassisName> **Cuda Chassis Manager**>**Configuration**> **Chassis Configuration**.
2. In the Summary window, select the chassis, slot, and interface that you wish to configure.
3. Click the **Agent Configuration** tab. The Agent Configuration window appears.
4. Click the **Groups** tab. The Groups window appears. Refer to Figure 7-8.

What You See

Figure 7-8 SNMP Groups window



Selected chassis / slot / interface: 113 / 13 / 0

Groups Rows: 5

Name	Context	Model	Level	Read View	Write View	Notify View
adc	adc	V1	NoAuth	public	private	public
adc	adc	V2c	NoAuth	public	private	public
adc	adc	V3	NoAuth	public	private	public
guitraps		V1	NoAuth			guitraps
guitraps		V2c	NoAuth			guitraps

Parameter Descriptions

This table provides a description of the Groups window parameters

Table 7-8 SNMP Groups Window Parameters.I

Parameter	Description
Name	Name of the group
Context	Name of the associated context
Model	Security model that processes SNMP messages. The options are V1, V2c, or V3.
Level	Minimum level of security necessary to gain access rights to the group. The options are: NoAuth, Auth, or Priv.
Read View	Authorizes read access to the group
Write View	Authorizes write access to the group
Notify View	Authorizes access for notifications.

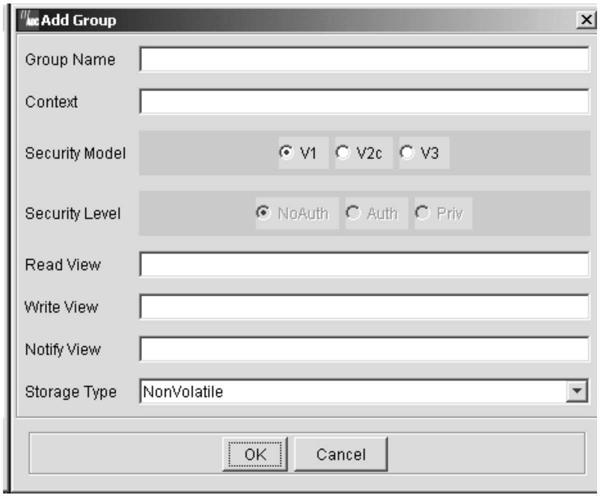
Adding SNMP Groups

Follow this procedure to add an SNMP group:

1. In the Groups window, click **Add**. The Add Group window appears.
2. Enter values for the parameters. Refer to Table 7-9.
3. Click **Ok** to add the group or click **Cancel** to return to the previous window.

What You See

Figure 7-9 Add Group window



Add Group

Group Name

Context

Security Model ● V1 ○ V2c ○ V3

Security Level ● NoAuth ○ Auth ○ Priv

Read View

Write View

Notify View

Storage Type NonVolatile

Note: In this example, v1 is set. No authentication or encryption is performed.

Parameter Descriptions

This table provides a description of the Add Groups window parameters

Table 7-9 SNMP Add Groups Window Parameters.

Parameter	**Description**
Group Name	Name of the group
Context	Name of the associated context
Security Model	Security model that processes SNMP messages. The options are V1, V2c, or V3.
Security Level	Security level necessary to gain access rights to the group. The options are: NoAuth (no Authentication), Auth (Authenticated), and Priv (Private).
Read View	Authorizes read access to the group
Write View	Authorizes write access to the group
Notify View	Authorizes access for notifications.
Storage Type	Storage type for this entry.
Volatile	Entry is stored in volatile memory. The information is lost during a system reboot.
Non-volatile	Entry is stored in non-volatile memory. The information is not lost during a system reboot.
Permanent	Entry is stored in non-volatile memory. You cannot delete the information but you can make modifications.
Read-only	Entry is stored in non-volatile memory. You cannot delete or modify the information.

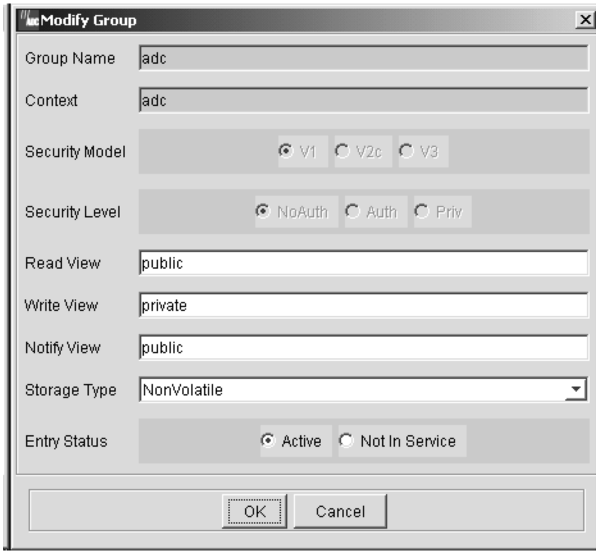
Modifying SNMP Groups

Follow this procedure to modify an SNMP group:

1. In the Groups window, select the group you wish to modify and click **Modify**. The Modify Group window appears.
2. Update the necessary information.
3. Click **Apply** to commit the changes or click **Cancel** to exit without saving.

What You See

Figure 7-10 Modify Group window



Modify Group

Group Name: adc

Context: adc

Security Model: ● V1 ○ V2c ○ V3

Security Level: ● NoAuth ○ Auth ○ Priv

Read View: public

Write View: private

Notify View: public

Storage Type: NonVolatile

Entry Status: ● Active ○ Not In Service

Deleting an SNMP Group

Follow this procedure to delete an SNMP group:

1. In the Groups window, select the group you with to delete and click **Delete**. A confirmation window appears.
2. Click **Yes** to delete the group or click **No** to cancel the deletion.

Configuring SNMP Access Views

You can configure views to determine whether a user can access a particular MIB subtree.

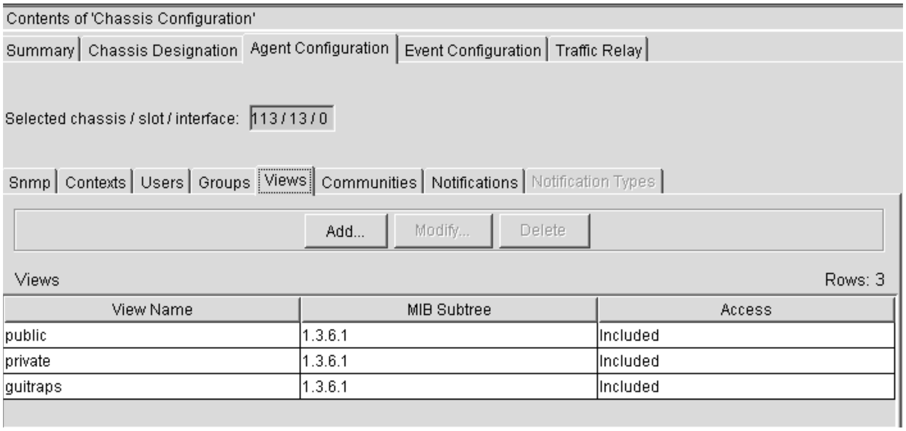
Before You Begin

Before you configure SNMP access views, follow this procedure:

1. Navigate to **Network Browser**>GroupName>ChassisName>**Cuda Chassis Manager**>**Configuration**>**Chassis Configuration.**
2. In the **Summary** tab, select the chassis, slot, and interface that you wish to configure.
3. Click the **Agent Configuration** tab. The Agent Configuration window appears.
4. Click the **Views** tab. The Views window appears.

What You See

Figure 7-11 Views window



Selected chassis / slot / interface: 113 / 13 / 0

Views Rows: 3

View Name	MIB Subtree	Access
public	1.3.6.1	Included
private	1.3.6.1	Included
guitraps	1.3.6.1	Included

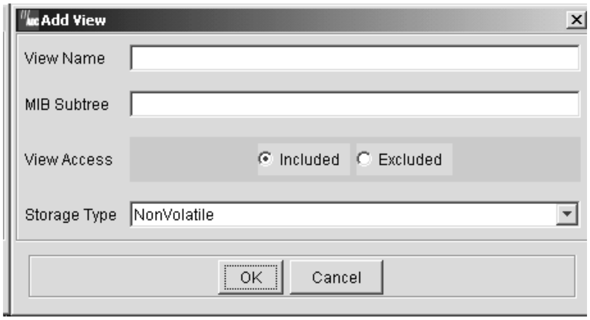
Adding an SNMP Access View

Follow this procedure to add an SNMP access view:

1. From the Views window, click **Add**. The Add View window appears.
2. Enter values for the parameters. Refer toTable 7-10.
3. Click **Ok** to add the access view or click **Cancel** to return to the previous window.

What You See

Figure 7-12 Add View window



Parameter Descriptions

This table provides a description of the Add View window

Table 7-10 SNMP Add View Window Parameters.

Parameter	Description
View Name	Name of the view. The range is 1 to 32 characters.
MIB Subtree	MIB subtree that defines the family of view subtrees. You can enter the MIB value in various formats. For example you can enter the MIB value as an Object Identifier (OID), an OID with wildcards, or an OID name description, such as, sysDescr.
View Access	Indicates whether the corresponding instances of the MIB subtree are Included or Excluded from the MIB view.
Storage Type	Storage type for this entry.
Volatile	Entry is stored in volatile memory. The information is lost during a system reboot.
Non-volatile	Entry is stored in non-volatile memory. The information is not lost during a system reboot.
Permanent	Entry is stored in non-volatile memory. You cannot delete the information but you can make modifications.
Read-only	Entry is stored in non-volatile memory. You cannot delete or modify the information.

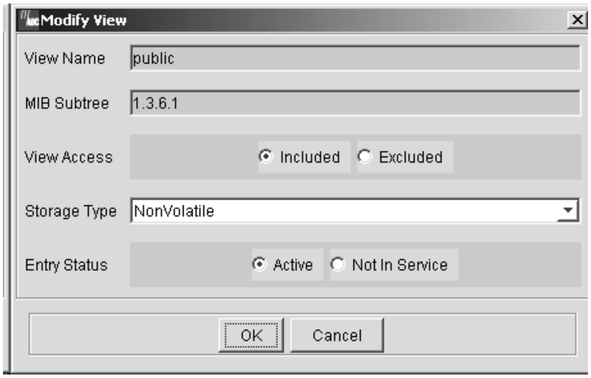
Modifying an SNMP Access View

Follow this procedure to modify an SNMP access view:

1. From the Views window, select the group you wish to modify.
2. Click **Modify**. The Modify View window appears.
3. Update the necessary information.
4. Click **Apply** to commit the changes or click **Cancel** to exit without saving.

What You See

Figure 7-13 Modify View window



View Name: public

MIB Subtree: 1.3.6.1

View Access: ● Included ○ Excluded

Storage Type: NonVolatile

Entry Status: ● Active ○ Not In Service

Parameter Descriptions

This table provides a description of the Modify View window.

Table 7-11 SNMP Modify View Window Parameters.

Parameter	**Description**
View Name	Name of the view. The range is 1 to 32 characters.
MIB Subtree	MIB subtree that defines the family of view subtrees. You can enter in the MIB value as an Object Identifier (OID), an OID with wildcards, or an OID name description, such as, sysDescr.
View Access	Indicates whether the corresponding instances of the MIB subtree are Included or Excluded from the MIB view.
Storage Type	Storage type for this entry.
Volatile	Entry is stored in volatile memory. The information is lost during a system reboot.
Non-volatile	Entry is stored in non-volatile memory. The information is not lost during a system reboot.
Permanent	Entry is stored in non-volatile memory. You cannot delete the information but you can make modifications.
Read-only	Entry is stored in non-volatile memory. You cannot delete or modify the information.
Entry Status	Allows you to enable or disable an entry.

Parameter	Description
Active	Activates an entry.
Not In Service	Disables the entry.

Deleting an SNMP Access View

Follow this procedure to delete an SNMP access view:

1. From the Views window, select the view you with to delete.
2. Click **Delete**. A confirmation window appears.
3. Click **Yes** to commit the changes or click **No** to cancel the deletion.

Configuring SNMP Communities

An SNMP community is a pairing of SNMP application and SNMP agent. The purpose of configuring a community is to differentiate access by context, group, and to control which hosts recognize the community string. You can view, add, modify, or delete SNMPv1 or SNMPv2c communities and any hosts given access to those communities.

SNMPv1 and SNMPv2c do not recognize context separately, but do recognize context when you have associated it with a Community, as described in the next procedure.

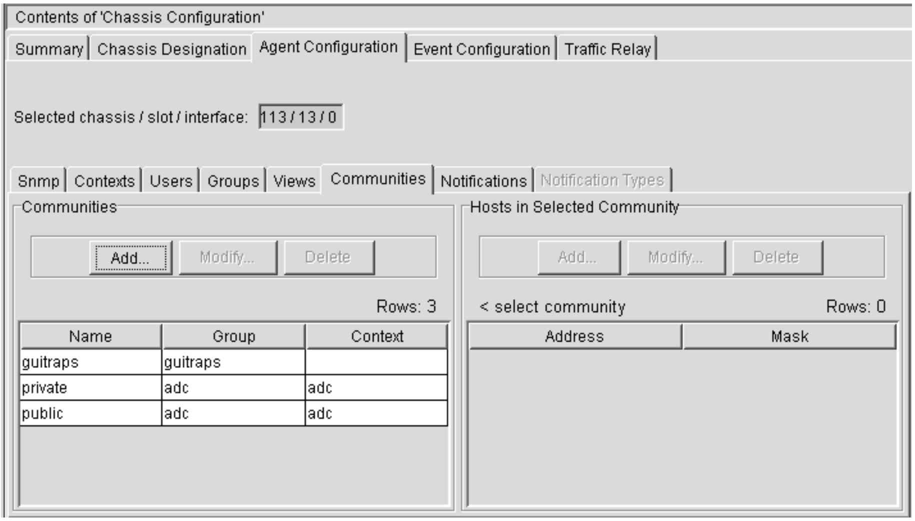
Before You Begin

Before you configure SNMP communities, follow this procedure:

1. Navigate to **Network Browser**>GroupName>ChassisName>**Cuda Chassis Manager**>**Configuration**>**Chassis Configuration.**
2. In the Summary window, select the chassis, slot, and interface that you wish to configure.
3. Click the **Agent Configuration** tab. The Agent Configuration window appears.
4. Click the **Communities** tab. The Communities window appears.
5. Click an entry in the Communities table. The hosts for the selected community appears in the Hosts in Selected Community table.

What You See

Figure 7-14 Communities window



Selected chassis / slot / interface: 113 / 13 / 0

Rows: 3

Name	Group	Context
guitraps	guitraps	
private	adc	adc
public	adc	adc

Rows: 0

Address	Mask

Parameter Descriptions

This table provides a description of the Communities window

Table 7-12 SNMP Communities Window Parameters.

Parameter	Description
Communities	Provides the defined communities
Name	The name for the specified community. The range is 1 to 32 characters.
Group	Group that associates with this community.
Context	Context that management information accesses when using the community string.
Hosts in Selected Communities	Provides the defined hosts for the selected community.
Address	The transport address. If you do not configure any hosts, all hosts are permitted. If this is the case, ANYHOST displays in the address column.

Parameter	Description
Mask	Mask value that associates this host with the group. The mask allows any host in a range. For example, 220.220.0.0 has a mask of 255.255.0.0. This allows any host from 220.220.0.0 through 220.220.255.255.

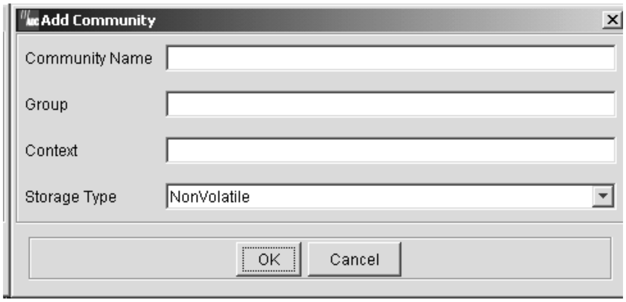
Adding an SNMP Community

Follow this procedure to add an SNMP community:

1. In the Communities window, click **Add** in the Communities table. The Add Community window appears.
2. Enter values for the parameters. Refer to ().
3. Click **Ok** to add the community or click **Cancel**.

What You See

Figure 7-15 Add Community window



Add Community

Community Name

Group

Context

Storage Type NonVolatile

Parameter Descriptions

This table provides a description of the Add Community window.

Parameter	Description
Community Name	Name of the community
Group	Name of the associated group.
Context	Name of the associated context.
Storage Type	Storage type for this entry.

Parameter	Description
Volatile	Entry is stored in volatile memory. The information is lost during a system reboot.
Non-volatile	Entry is stored in non-volatile memory. The information is not lost during a system reboot.
Permanent	Entry is stored in non-volatile memory. You cannot delete the information but you can make modifications.
Read-only	Entry is stored in non-volatile memory. You cannot delete or modify the information.

Modifying an SNMP Community

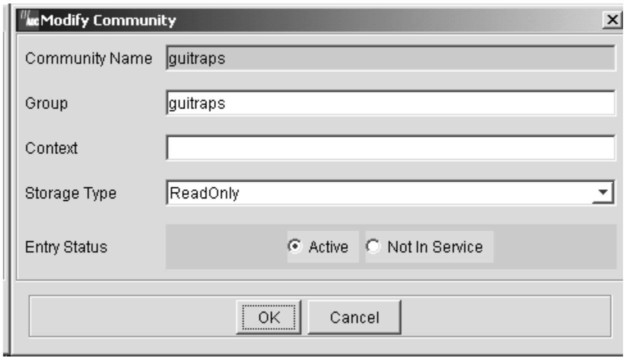
Follow this procedure to modify an SNMP community:

1. In the Communities window, select the community you wish to modify in the Communities table.
2. Click **Modify**. The Modify Community window appears.
3. Update the necessary information.
4. Click **Ok** to commit the changes or click **Cancel** to exit without saving.

What You See

This figure shows an example of the Modify Community window

Figure 7-16 Modify Community Window



Modify Community

Community Name: guitraps

Group: guitraps

Context:

Storage Type: ReadOnly

Entry Status: ● Active ○ Not In Service

Parameter Descriptions

This table provides a description of the Modify Community window

Table 7-13 SNMP Modify Community Window Parameters.

Parameter	Description
Community Name	Name of the community
Group	Name of the associated group.
Context	Name of the associated context.
Storage Type	Storage type for this entry.
Volatile	Entry is stored in volatile memory. The information is lost during a system reboot.
Non-volatile	Entry is stored in non-volatile memory. The information is not lost during a system reboot.
Permanent	Entry is stored in non-volatile memory. You cannot delete the information but you can make modifications.
Read-only	Entry is stored in non-volatile memory. You cannot delete or modify the information.
Entry Status	Allows you to enable or disable an entry.
Active	Activates an entry.

Parameter	Description
Not In Service	Disables the entry.

Deleting an SNMP Community

Follow this procedure to delete an SNMP community:

1. In the Communities window, select the community you wish to delete in the Communities table.
2. Click **Delete**. A confirmation window appears.
3. Click **Ok** to commit the changes or click **Cancel** to cancel the deletion.

Adding an SNMP Host

SNMP hosts receive event notifications. The SNMP host may be the default local host on the management module, or an external host that you configure to receive the notifications.

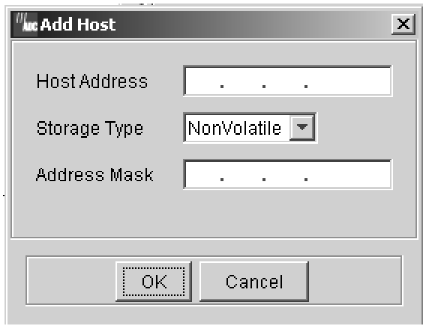
The local host is the default host that is pre-configured and shipped with your chassis.Notifications, for the local host, are sent to IP address 127.0.0.1. If CudaView is installed on the chassis, CudaView uses the local host to display notifications. The local host IP address should not be changed.

Follow this procedure to add an SNMP host:

1. In the Communities window, select the community in the Communities table for which you wish to add a host
2. In the Hosts in Selected Community table, click **Add**. The Add Host window appears.
3. Enter values for the parameters. Refer to Table 7-14.
4. Click **Ok** to add the community or click **Cancel** to exit without saving.

What You See

Figure 7-17 Add Host window



Add Host

Host Address . . .

Storage Type NonVolatile

Address Mask . . .

Parameter Descriptions

This table provides a description of the Add Host window

Table 7-14 SNMP Add Host Window Parameters.

Parameter	Description
Host Address	The host IP address.
Storage Type	Storage type for this entry.
Volatile	Entry is stored in volatile memory. The information is lost during a system reboot.
Non-volatile	Entry is stored in non-volatile memory. The information is not lost during a system reboot.
Permanent	Entry is stored in non-volatile memory. You cannot delete the information but you can make modifications.
Read-only	Entry is stored in non-volatile memory. You cannot delete or modify the information.
Address Mask	Mask value that associates this host with the group. The mask allows any host in a range. For example, 220.220.0.0 has a mask of 255.255.0.0. This allows any host from 220.220.0.0 through 220.220.255.255.

Modifying an SNMP Host

Follow this procedure to modify an SNMP host:

1. In the Communities window, select the community in the Hosts in Selected Community table you wish to modify. Click **Modify**. The Modify Community window appears.
2. Update the necessary information.
3. Click **Ok** to commit the changes or click **Cancel** to exit without saving.

Deleting an SNMP Host

Follow this procedure to delete an SNMP host:

1. In the Communities window, select the host in the Communities table for which you wish to delete a host
2. In the Hosts in Selected Community table, select the host you wish to delete and click **Delete**. A confirmation window appears.
3. Click **Ok** to commit the changes or click **Cancel** to cancel the deletion.

Configuring SNMP Notifications

Notifications indicate that a system event occurred, such as a physical fault that affects the chassis, and system faults that may impact the operation of the management module or any of the application modules. For information about SNMP hosts, refer to section "Adding an SNMP Host" on page 156.

Notifications are sent to an SNMP host. Configuring event notification involves defining which SNMP host receives the notifications and how the notifications are sent to the SNMP host.

Notifications may be sent as traps or informs. Traps are notifications that are not acknowledged by the SNMP manager, so they are considered unreliable. In addition, traps are not held in memory. Informs are notifications that are acknowledged by the SNMP manager, so they are considered reliable. If an inform is sent and not acknowledged, it may be sent again. Informs are held in memory, which means they consume more router and network resources.

You can view, add, modify, or delete SNMP notifications. Follow these procedures to configure SNMP notifications.

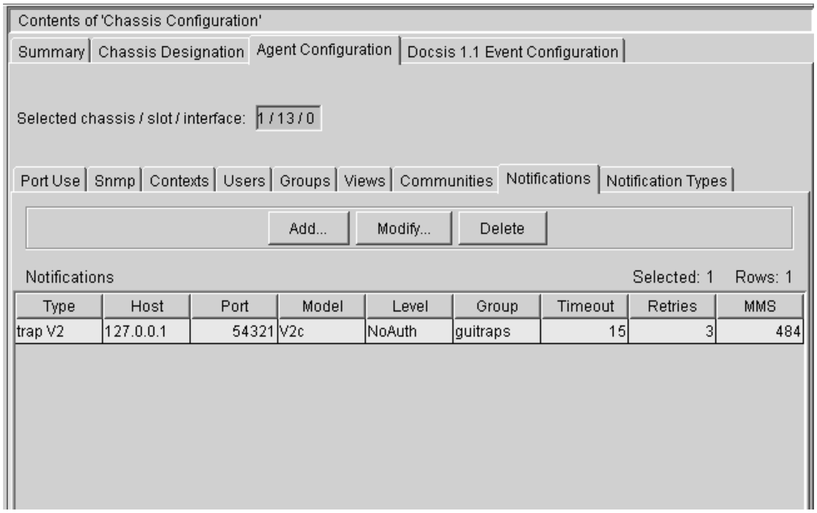
Before You Begin

Before you configure SNMP notifications, follow this procedure:

1. Navigate to **Network Browser**>GroupName>ChassisName> **Cuda Chassis Manager**>**Configuration**>**Chassis Configuration.**
2. In the Summary window, select the chassis, slot, and interface that you want to configure.
3. Click the **Agent Configuration** tab. The Agent Configuration window appears.
4. Click the **Notifications** tab. The Notifications window appears.

What You See

Figure 7-18 Notifications window.



Selected chassis / slot / interface: 1 / 13 / 0

Selected: 1 Rows: 1

Type	Host	Port	Model	Level	Group	Timeout	Retries	MMS
trap V2	127.0.0.1	54321	V2c	NoAuth	guitraps	15	3	484

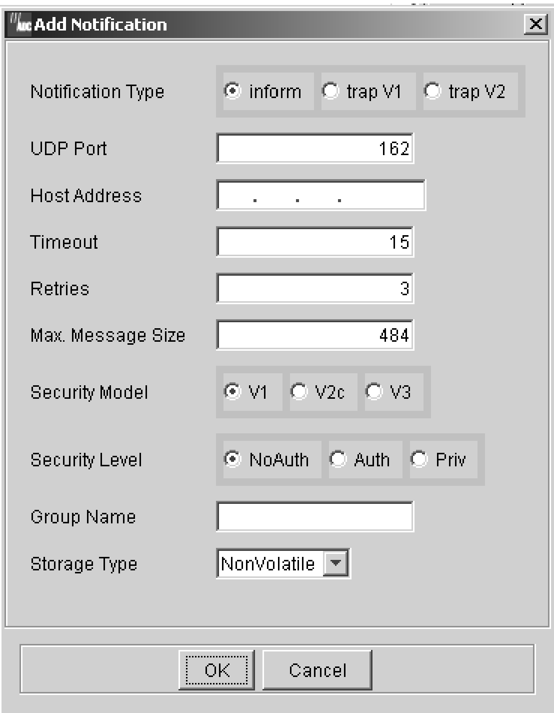
Adding an SNMP Notification

Follow this procedure to add an SNMP notification:

1. In the Notifications window, click **Add**. The Add Notifications window appears.
2. Enter values for the parameters. Refer to Table 7-15.
3. Click **Ok** to add the notification or click **Cancel** to exit without saving.

What You See

Figure 7-19 Add Notifications window



Notification Type ● inform ○ trap V1 ○ trap V2

UDP Port 162

Host Address . . .

Timeout 15

Retries 3

Max. Message Size 484

Security Model ● V1 ○ V2c ○ V3

Security Level ● NoAuth ○ Auth ○ Priv

Group Name

Storage Type NonVolatile

Parameter Descriptions

This table provides a description of the Add Notifications window

Table 7-15 SNMP Add Notification Window Parameters.

Parameter	Description
Notification Type	Type of notification for this entry. The options are:
inform	Any messages generated contain confirmed PDUs
trap V1	Any messages generated contain unconfirmed PDUs.
trap V2	Any messages generated contain unconfirmed PDUs.
UDP Port	Port to which the notification is sent.
Host Address	IP address of the host.

Parameter	Description
Timeout	Amount of time that passes before it is assumed the host did not receive the notification message.
Retries	When the notification type is set to Inform, the Retries parameter indicates the number of retries made when a response is not received for a generated message. The range is 0 to 255 and the default is 3.
Max. Message Size	Maximum message size of an SNMP message that the SNMP engine transmits or receives and processes.
Security Model	Security model that processes SNMP messages. The options are V1, V2c, or V3.
Security Level	Minimum level of security to necessary to gain access rights. The options are: NoAuth (no Authentication), Auth (Authenticated), and Priv (encryption). The default is NoAuth.
Group Name	Name of the associated group.
Storage Type	Storage type for this group.
Volatile	Entry is stored in volatile memory. The information is lost during a system reboot.
Non-volatile	Entry is stored in non-volatile memory. The information is not lost during a system reboot.
Permanent	Entry is stored in non-volatile memory. You cannot delete the information but you can make modifications.
Read-only	Entry is stored in non-volatile memory. You cannot delete or modify the information.

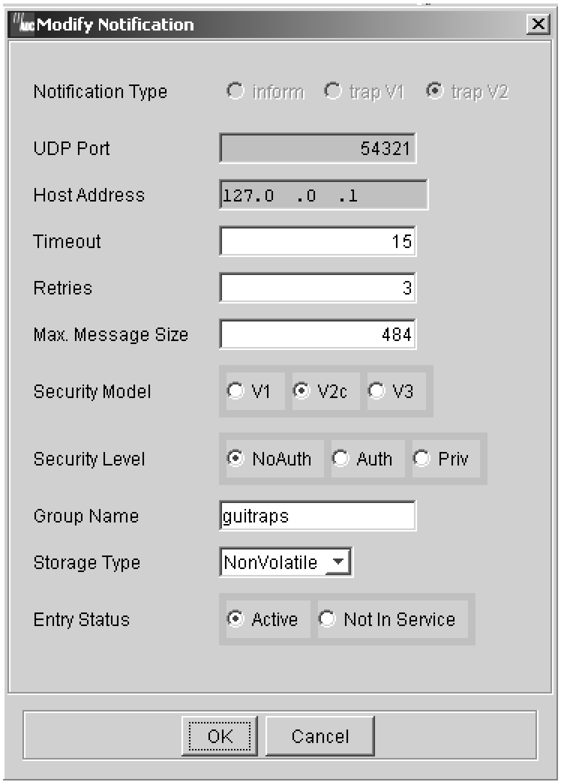
Modifying an SNMP Notification

Follow this procedure to modify an SNMP notification:

1. In the Notifications window, select the notification you wish to modify and click **Modify**. The Modify Notification window appears.
2. Update the necessary information. Refer to Table 7-15.
3. Click **Ok** to commit the changes or click **Cancel** to exit without saving.

What You See

Figure 7-20 Modify Notification window



Modify Notification

Notification Type ○ inform ○ trap V1 ● trap V2

UDP Port 54321

Host Address 127.0 .0 .1

Timeout 15

Retries 3

Max. Message Size 484

Security Model ○ V1 ● V2c ○ V3

Security Level ● NoAuth ○ Auth ○ Priv

Group Name guitraps

Storage Type NonVolatile

Entry Status ● Active ○ Not In Service

Deleting an SNMP Notification

Follow this procedure to delete an SNMP notification:

1. In the Notifications window, select the notification you wish to delete and click **Delete**. A confirmation window appears.
2. Click **Yes** to commit the changes or click **No** to cancel the deletion.

Selecting SNMP Notification Types

Notifications types are specific faults associated to system operations. The Cuda 12000 supports notification types for the following system operations:

- Cluster
- Module
- Interface
- DOCSIS
- Routing
- Provisioning *(Provisioning-related faults are supported only if you are using the FastFlow Broadband Provisioning Manager (FastFlow BPM.)*

Notification types are sent to the SNMP Hosts that are configured to receive SNMP Notifications. (**NOTE:** You must configure SNMP Notifications before you select SNMP Notification Types.) Notification types are associated with system event levels. The Cuda 12000 supports the following event levels:

- Critical
- Warning
- Notice
- Error
- Informational

For more information about event levels, refer to Chapter 8, “Managing System Events”.

This section describes the notification types and explains how to select notification types for system operations.

Before You Begin

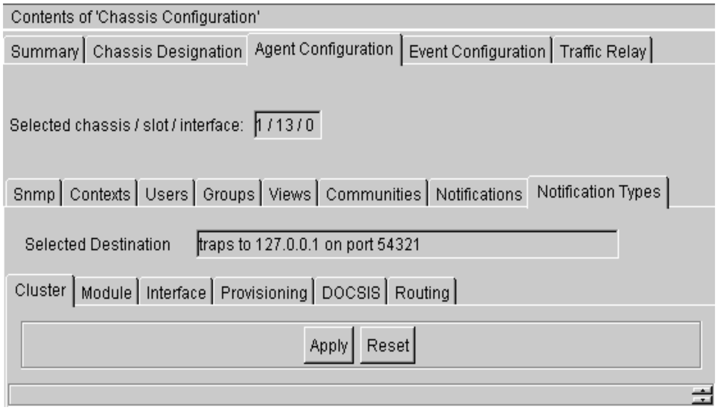
Before you configure SNMP Notification Types, follow this procedure:

1. Navigate to **Network Browser**>GroupName>ChassisName> **Cuda Chassis Manager**>**Configuration**>**Chassis Configuration.**
2. In the Summary window, select the chassis, slot, and interface that you want to configure.

3. Click the **Agent Configuration** tab. The Agent Configuration window appears.
4. Click the **Notifications** tab. The Notifications window appears.
5. Select the row that includes the SNMP Host that you want to receive notifications.
6. Click the **Notifications Types** tab. The Notifications Types window appears. Figure 7-21 displays the tabs for the system operations.

The fault information for each system operation is explained in the appropriate sections that follow.

Figure 7-21 SNMP Notification Types Tab Display



Selected chassis / slot / interface: 1 / 13 / 0

Selected Destination: traps to 127.0.0.1 on port 54321

Selecting Cluster-related Notification Types

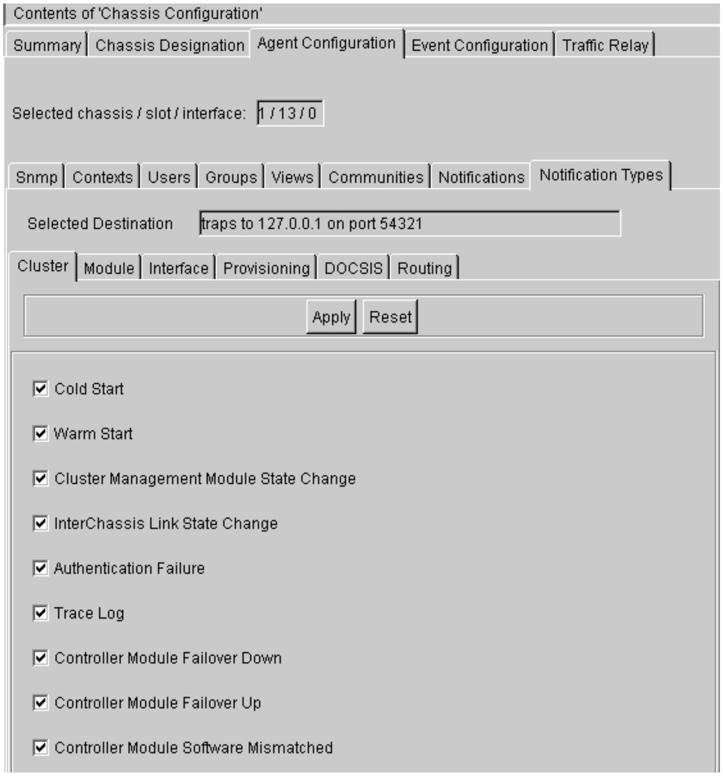
Cluster notification types refer to faults that affect the management module.

Follow this procedure to select notification types for cluster-related system operations:

1. In the Notifications Types window, click the **Cluster** tab. The Cluster window appears.
2. Select the notification types for which you want to be notified. Refer to Table 7-16.
3. Click **Apply** to commit the changes or click **Reset** to return to default values.

What You See

Figure 7-22 Cluster Window



Selected chassis / slot / interface: 1 / 13 / 0

Selected Destination: traps to 127.0.0.1 on port 54321

☑ Cold Start

☑ Warm Start

☑ Cluster Management Module State Change

☑ InterChassis Link State Change

☑ Authentication Failure

☑ Trace Log

☑ Controller Module Failover Down

☑ Controller Module Failover Up

☑ Controller Module Software Mismatched

Parameter Descriptions

This table provides a description of the Cluster-related notification types and associated event levels.

Table 7-16 Cluster-related SNMP Notification Types.

Parameter	Description	Event Level
Cold Start	Module boots from power up.	Notice
Warm Start	Module boots from reset.	Notice
Cluster Management Module State Change	A change in the craft port IP address.	Notice
InterChassis Link State Change	A change in the ICL link.	Notice

Parameter	Description	Event Level
Authentication Failure	SNMP receives a bad Community Name.	Notice
Trace Log	*For ADC internal use only.*	Notice
Controller Module Failover Down	Redundancy services are going down. This notification type applies to only redundant configurations.	Notice
Controller Module Failover Up	Redundancy services are up. This notification type applies to only redundant configurations.	Notice
Controller Module Software Mismatched	The secondary module does not come up because its software revision does not match the software revision of the primary module. This notification type applies to only redundant configurations.	Notice

Selecting Module-related Notification Types

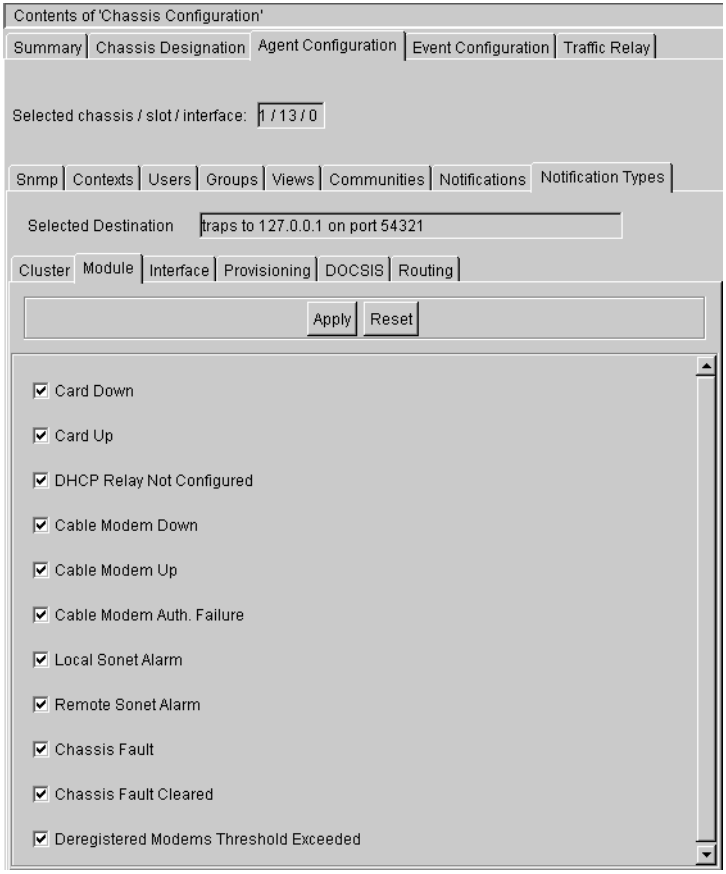
Module notification types refer to hardware faults that affect any application module.

Follow this procedure to select the notifications for module-related system operations:

1. In the Notifications Type window, click the **Module** tab. The Module window appears.
2. Select the notification types for which you want to be notified. Refer to Table 7-17.
3. Click **Apply** to commit the changes or click **Reset** to return to default values.

What You See

Figure 7-23 Module Window



Selected chassis / slot / interface: 1 / 13 / 0

Selected Destination: traps to 127.0.0.1 on port 54321

- ☑ Card Down
- ☑ Card Up
- ☑ DHCP Relay Not Configured
- ☑ Cable Modem Down
- ☑ Cable Modem Up
- ☑ Cable Modem Auth. Failure
- ☑ Local Sonet Alarm
- ☑ Remote Sonet Alarm
- ☑ Chassis Fault
- ☑ Chassis Fault Cleared
- ☑ Deregistered Modems Threshold Exceeded

Parameter Descriptions

This table provides a description of the Module-related notification types and associated event levels.

Table 7-17 Module-related SNMP Notifications Types.

Parameter	Description	Event Level
Card Down	Module failure.	Critical

Parameter	Description	Event Level
Card Up	Module is operating normally.	Notice
DHCP Relay Not Configured	DHCP configuration error.	Warning
Cable Modem Down	Cable modem is not operational.	Critical
Cable Modem Up	Cable modem is operating normally.	Notice
Cable Modem Auth. Failure	Cable modem failed authorization and did not register.	Notice
Local Sonet Alarm	Transmission problem is detected from the transmitter.	Error
Remote Sonet Alarm	A transmission problem is detected from the receiver.	Error
Chassis Fault	A fault in an auxiliary device. For information on auxiliary device faults, see Chapter 11, “Fault Management”.	Critical
Chassis Fault cleared	A fault in an auxiliary device has been cleared.	Notice
Deregistered Modems Threshold Exceeded	Signifies that a number of percentage of modems have deregistered over the deregistration time interval.	Warning

Selecting Interface-related Notification Types

Interface notification types refer to faults that affect the link state of the interface.

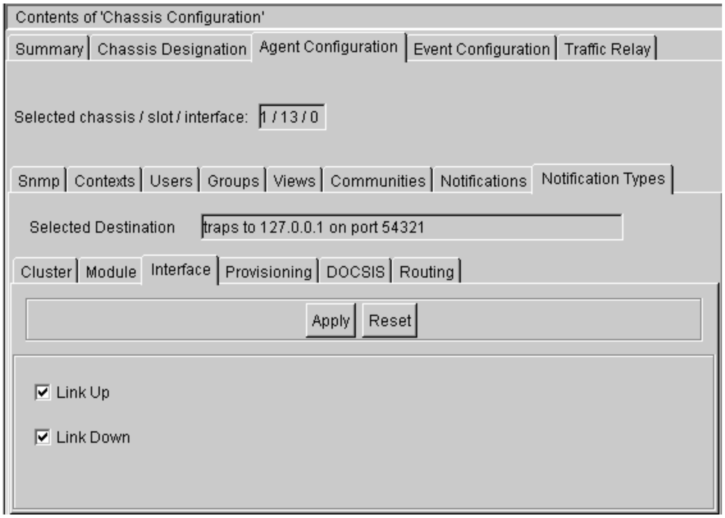
Follow this procedure to select the notifications for interface-related system operations:

1. In the Notifications window, click the **Interface** tab. The Interface window appears.
2. Select the notification types for which you want to be notified. Refer to Table 7-18.
3. Click **Apply** to commit the changes or click **Reset** to return to default values.

What You See

This figure shows an example of the Interface window.

Figure 7-24 Interface Window



Contents of 'Chassis Configuration'

Selected chassis / slot / interface: 1 / 13 / 0

Selected Destination: traps to 127.0.0.1 on port 54321

☑ Link Up

☑ Link Down

Parameter Descriptions

This table provides a description of the Interface-related notification types and associated event levels.

Table 7-18 SNMP Interface-related Notification Types Window.

Parameter	Description	Event Level
Link Up	Link to IP network is operating normally.	Notice

Parameter	Description	Event Level
Link Down	Link to IP network is not functioning.	Error

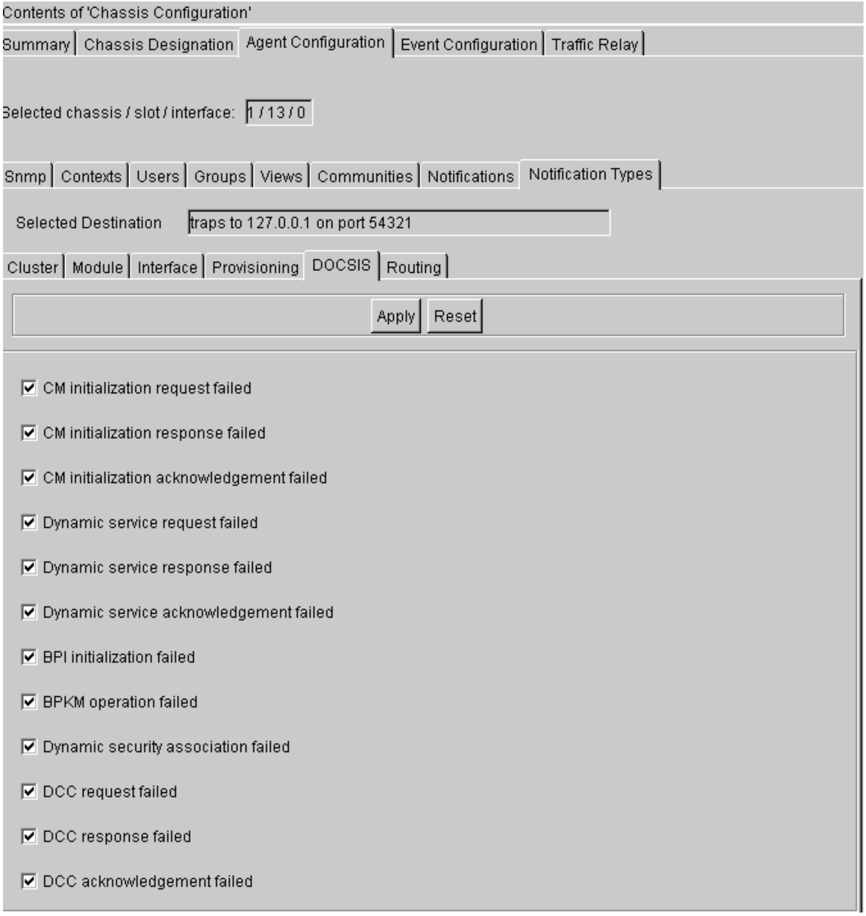
Selecting DOCSIS/EuroDOCSIS-related Notification Types

DOCSIS notification types refer to initialization faults on DOCSIS and EuroDOCSIS modules.

Follow this procedure to select the notifications for DOCSIS/EuroDOCSIS-related system operations:

1. In the Notifications window, click the **DOCSIS** tab. The DOCSIS window appears.
2. Select the notification types for which you want to be notified. Refer to Table 7-19.
3. Click **Apply** to commit the changes or click **Reset** to return to default values.

Figure 7-25 DOCSIS Window



Selected chassis / slot / interface: 1 / 13 / 0

Selected Destination: traps to 127.0.0.1 on port 54321

☑ CM initialization request failed

☑ CM initialization response failed

☑ CM initialization acknowledgement failed

☑ Dynamic service request failed

☑ Dynamic service response failed

☑ Dynamic service acknowledgement failed

☑ BPI initialization failed

☑ BPKM operation failed

☑ Dynamic security association failed

☑ DCC request failed

☑ DCC response failed

☑ DCC acknowledgement failed

This table provides a description of the DOCSIS/EuroDOCSIS-related notification types and associated event levels.

Table 7-19 DOCSIS-related Notification Types

Parameter	Description	Event Level
CM Initialization Request Failed	A registration request failure from the cable modem occurred during the cable modem initialization process and was detected on the CMTS side.	Warning

Parameter	Description	Event Level
CM Initialization Response Failed	A registration response failure from the cable modem occurred during the cable modem initialization process and was detected on the CMTS side.	Warning
CM Initialization Acknowledgment Failed	A registration acknowledgement failure from the cable modem occurred during the cable modem initialization process and was detected on the CMTS side.	Warning
Dynamic Service Request Failed	A dynamic service request failure occurred during the dynamic services process.	Warning
Dynamic Service Response Failed	A dynamic service response failure occurred during the dynamic services process.	Warning
BPI Initialization Failed	A BPI initialization attempt failure occurred during the registration process.	Informational
BPKM Operation Failed	A baseline privacy key management operation failed.	Error
Dynamic Security Association Failed	A dynamic security association failed.	Warning
DCC Request Failed	A dynamic channel change request failure occurred during the dynamic channel change process on the cable modem side.	Warning
DCC Response Failed	A dynamic channel change response failure occurred during the dynamic change process on the cable modem side.	Warning
DCC Acknowledge Failed	A dynamic channel change acknowledgment failure occurred during the dynamic channel change process on the cable modem side.	Warning

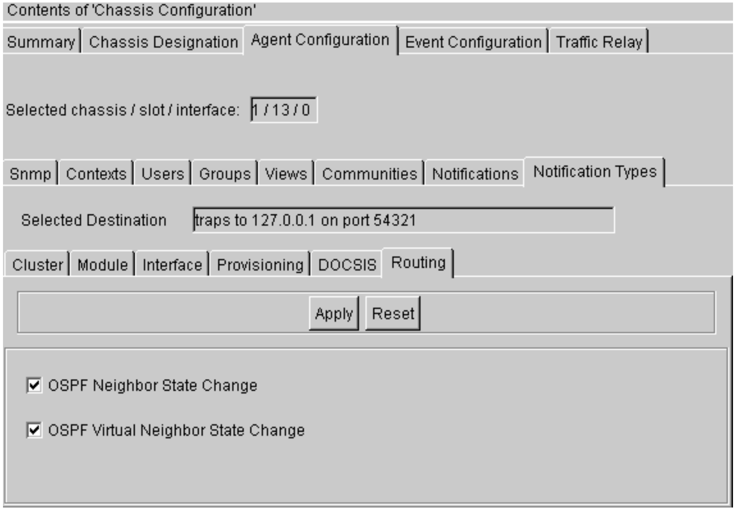
Selecting Routing-related Notification Types

Routing notification types refer to faults that indicate a change in the state of OSPF neighbors and OSPF virtual neighbors.

Follow this procedure to select the notifications for Routing-related system operations:

1. In the Notifications window, click the **Routing** tab. The Routing window appears.
2. Select the notification types for which you want to be notified. Refer to Table 7-20.
3. Click **Apply** to commit the changes or click **Reset** to return to default values.

Figure 7-26 Routing Window



Selected chassis / slot / interface: 1 / 13 / 0

Selected Destination: traps to 127.0.0.1 on port 54321

☑ OSPF Neighbor State Change

☑ OSPF Virtual Neighbor State Change

This table provides a description of the Routing-related notification types and associated event levels:

Table 7-20 Routing-related Notification Types.

Parameter	Description	Event Level
OSPF Neighbor State Change	Signifies a change in the state of an OSPF neighbor on a physical interface.	Notice

Parameter	Description	Event Level
OSPF Virtual Neighbor State Change	Signifies a change in the state of an OSPF neighbor on a virtual interface.	Notice

Selecting Provisioning-related Notification Types

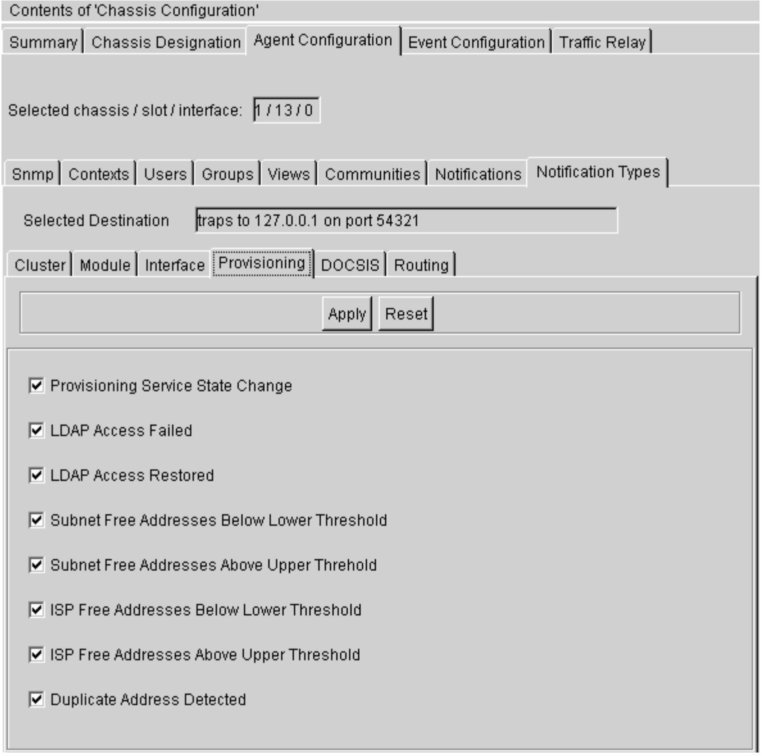
Provisioning notification types refer to faults that pertain to the FastFlow Broadband Provisioning Manager (FastFlow BPM). The Cuda 12000 supports provisioning notification types only if FastFlow BPM is running on the Cuda 12000.

NOTE: *If your Cuda 12000 is not running FastFlow BPM, CudaView does not display the Provisioning notification types tab*.

Follow this procedure to select the notifications for Provisioning-related system operations:

1. In the Notifications window, click the **Provisioning** tab. The Provisioning window appears.
2. Select the notification types for which you want to be notified. Refer to Table 7-20.
3. Click **Apply** to commit the changes or click **Reset** to return to default values.

Figure 7-27 Provisioning Window



Contents of 'Chassis Configuration'

Selected chassis / slot / interface: 1 / 13 / 0

Selected Destination traps to 127.0.0.1 on port 54321

☑ Provisioning Service State Change

☑ LDAP Access Failed

☑ LDAP Access Restored

☑ Subnet Free Addresses Below Lower Threshold

☑ Subnet Free Addresses Above Upper Threhold

☑ ISP Free Addresses Below Lower Threshold

☑ ISP Free Addresses Above Upper Threshold

☑ Duplicate Address Detected

This table provides a description of the Provisioning-related notification types and associated event levels:

Table 7-21 Provisioning-related Notification Types

Parameter	Description	Event Level
Provisioning Service State Change	A FastFlow BPM service started, stopped or failed.	Notice
LDAP Access Failed.	A directory server access failure occurred.	Notice
LDAP Access Restored.	A directory server access is operational after a failure.	Notice
Subnet Free Addresses Below Lower Threshold	The free address count fell below the lower threshold for the specified subnet.	Notice

Parameter	Description	Event Level
Subnet Free Addresses Above Upper Threshold	The free IP address count exceeded the higher available address threshold for the specified subnet.	Notice
ISP Free Addresses Below Lower Threshold	The free address count fell below the lower threshold for the specified ISP.	Notice
ISP Free Addresses ABove Upper Threshold	The free IP address count exceeded the higher available address threshold for the specified ISP.	Notice
Duplicate Address Detected	A duplicate IP address is detected.	Notice

8 MANAGING SYSTEM EVENTS

This chapter describe how to manage event transmission and includes the following sections:

- About System Events
- Configuring the Event Transmission
- Configuring Event Reporting
- Event Levels and SNMP Notification Types
- Viewing the Events
- Clearing the Event Log

About System Events

An event is a problem, a configuration change or some other noteworthy incident that occurs on the Cuda 12000 or in the network. Events create the generation of:

- System log (syslog) messages
- SNMP traps, which the Cuda 12000 sends to network management stations (configured as SNMP Hosts)
- Internal log messages

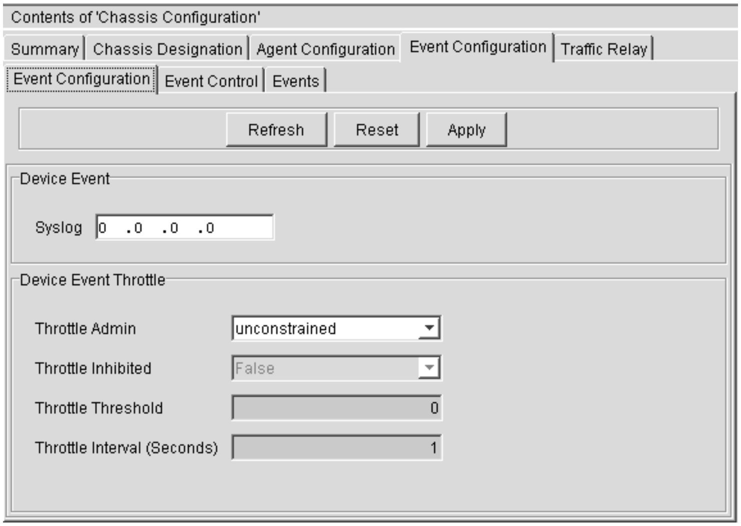
Before You Begin

Before you configure system events, follow this procedure:

1. Navigate to **Network Browser**>GroupName>ChassisName>**Cuda Chassis Manager**>**Configuration** > **Chassis Configuration.**
2. Click the **Event Configuration** tab. The Event Configuration window appears.

What You See

Figure 8-1 Event Configuration window



Syslog 0 .0 .0 .0

Throttle Admin unconstrained

Throttle Inhibited False

Throttle Threshold 0

Throttle Interval (Seconds) 1

Configuring the Event Transmission

A Cuda 12000 can generate a significant volume of events in a short period of time. The Cuda 12000 manages event transmission in compliance with DOCSIS 1.1 standards.

To avoid flooding the syslog server and network management stations with events, you can control the pace of event transmission by configuring the following parameters:

Parameter Descriptions

This table provides a description of the Event Configuration window.

Table 8-1 .Event Configuration Window Parameters

Parameter	Description
Syslog	IP address of the Syslog server. If a Syslog server IP address does not currently exist, the default is 0.0.0.0
Throttle Admin	Controls the transmission of traps and syslog messages with respect to the event threshold. Specify one of these administrative status values: ■ unconstrained (default) — The Cuda 12000 transmits traps and syslog messages without regard to the event threshold and interval settings. ■ maintainBelowThreshold — The Cuda 12000 suppresses traps and syslog messages if the number of events exceeds the threshold. ■ stopAtThreshold — The Cuda 12000 stops trap transmissions and syslog messages at the threshold. ■ inhibited – The Cuda 12000 suppresses all trap transmissions and syslog messages.
Throttle Inhibited	Displays the throttle inhibited status. This field displays True if one of the following conditions is met: ■ Throttle Admin is set to inhibited. ■ Throttle Admin is set to stopAtThreshold and the threshold has been reached. Otherwise, this field displays False.

Parameter	Description
Throttle Threshold	Read only. Number of events that the Cuda 12000 may generate per event interval before throttling occurs. Throttling is the process of eliminating excessive events. Note that an event causing both a trap and a syslog message is still treated as a single event. Values range from 0 to 4294967295. The default is 0.
Throttle Interval (Seconds)	Read only. The interval, in seconds, over which the event threshold applies. For example, if you configure an event threshold of 20 and an event interval of 40 seconds, then the Cuda 12000 may generate 20 events over 40 seconds before throttling occurs. Values range from 0 seconds to 2147483647 seconds. The default is 1.

Before you manage event transmission or reporting using the syslog server, you set the IP address of the syslog server to which your Cuda 12000 writes system log messages, as required by DOCSIS 1.1 standards. You may specify the IP address of the local Syslog server on your Cuda 12000 or a remote syslog server on another Cuda 12000.

To configure event transmission, follow this procedure:

1. In the Event Configuration window, click the **Event Configuration** tab.
2. Enter values for the parameters. (Refer to Table 8-1.)
3. Click **Apply** to commit the information or click **Reset** to return to the previous values.
4. Click **Refresh** to update the information.

Configuring Event Reporting

Each Cuda 12000 event belongs to one of eight event levels. An event level defines the severity of the event. You can configure each event level to be sent through a subset of reporting mechanisms (trap, syslog, or local event log). To do this, you specify:

- An event level
- How you want events in that level to be reported

Event Levels

Event levels are ordered from most critical (emergency) to least critical (debug). The following table lists the event level, in priority order:

Table 8-2 Event Level

Event Level	Description
Emergency	Indicates hardware- or software-related problems with DOCSIS or EuroDOCSIS modules. Prevents CMTS operation.
Alert	Indicates a serious failure that causes the Cuda 12000 to reboot.
Critical	Indicates a serious failure that requires attention and prevents the device from transmitting data. Failure may be resolved without a system reboot.
Error	Indicates a failure occurred that could interrupt the normal data flow.
Warning	Indicates a failure occurred that could interrupt the normal data flow. (This failure is not as severe as reported for Error events.)
Notice	Indicates an event that requires attention, but is not a failure.
Information	Indicates an event that may be helpful for tracing normal operation. Informational events do not report failures.
Debug	An event used for only debugging purposes.

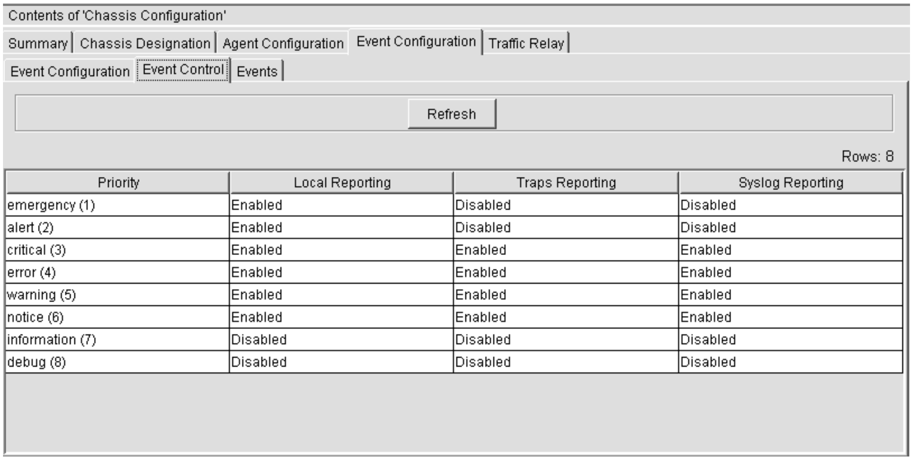
Viewing Event Levels

To view event levels, follow this procedure:

1. In the Event Configuration window, click the **Event Control** tab.
2. Click **Refresh** to update the information.

What You See

Figure 8-2 Event Control window



Rows: 8

Priority	Local Reporting	Traps Reporting	Syslog Reporting
emergency (1)	Enabled	Disabled	Disabled
alert (2)	Enabled	Disabled	Disabled
critical (3)	Enabled	Enabled	Enabled
error (4)	Enabled	Enabled	Enabled
warning (5)	Enabled	Enabled	Enabled
notice (6)	Enabled	Enabled	Enabled
information (7)	Disabled	Disabled	Disabled
debug (8)	Disabled	Disabled	Disabled

Reporting Actions

Each event level is associated with a reporting action or a combination of reporting actions. The following table lists the reporting actions that are supported by the Cuda 12000. Notice that Local is a required reporting action, within a combination of reporting actions:

Table 8-3 Reporting Actions

Reporting Action	Description
local	Write a message to the internal log.
local|traps	Write a message to the internal log and send a trap.
local|syslog	Write a message to the internal log and send a syslog message.

Reporting Action	Description
local|traps|syslog	Write a message to the internal log, send a trap, and send a syslog message.

By default, the Cuda 12000 reports events as follows:

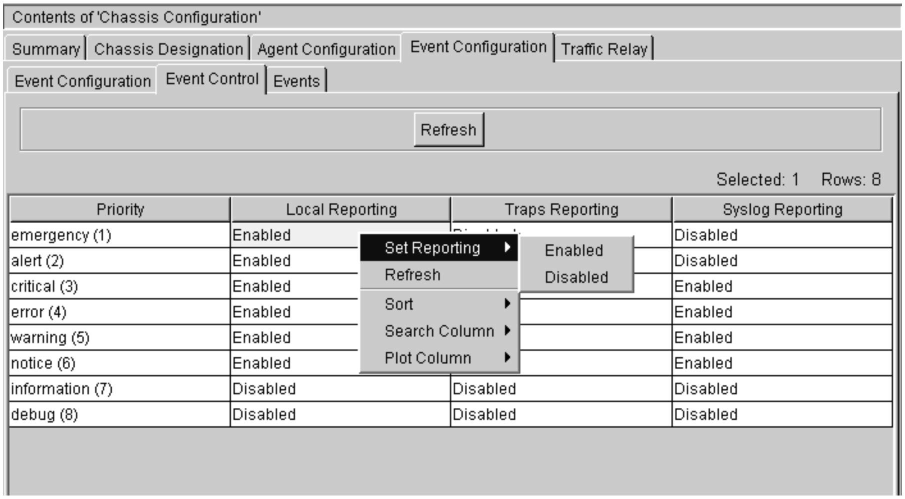
Table 8-4 Default Event Level Reporting Actions

Event Level	Default Reporting Action
Emergency	local
Alert	local
Critical	local|traps|syslog
Error	local|traps|syslog
Warning	local|traps|syslog
Notice	local|traps|syslog
Information	none
Debug	none

To configure reporting actions for the associated event levels, follow the procedure below. Table 8-3, “Reporting Actions” indicates the combination of reporting actions that are supported by the Cuda 12000.

1. In the Event Configuration window, click the **Event Control** tab.
2. Within the Priority column, go to the event level for which you want to configure a reporting action.
3. In the same row of the specific event level, select the reporting action that you want to configure and right-click. A sub-menu is displayed. (Refer to Figure 8-3.)
4. Choose Enabled to assign the reporting action to the event level; or, choose Disabled to remove the reporting action from the event level. **Note:** Traps and/or Syslog must be disabled before you can set Local to Disabled.
5. Repeat step 3 and 4 for each reporting action you want to configure for the specific event level.

Figure 8-3 Set Reporting Sub-menu



Selected: 1 Rows: 8

Priority	Local Reporting	Traps Reporting	Syslog Reporting
emergency (1)	Enabled		Disabled
alert (2)	Enabled		Disabled
critical (3)	Enabled		Enabled
error (4)	Enabled		Enabled
warning (5)	Enabled		Enabled
notice (6)	Enabled		Enabled
information (7)	Disabled	Disabled	Disabled
debug (8)	Disabled	Disabled	Disabled

Figure 8-3 is an example of the sub-menu to configure the Local reporting action for the Emergency event level.

Event Levels and SNMP Notification Types

Event levels are associated with SNMP Notification Types for the following system operations:

- Cluster
- Module
- Interface
- DOCSIS
- Routing
- Provisioning *(Provisioning-related faults are supported only if you are using the FastFlow Broadband Provisioning Manager (FastFlow BPM.)*

For additional information about SNMP Notification Types and associated event levels, refer to Chapter 7, “Simple Network Management Protocol (SNMP)” on page 125.

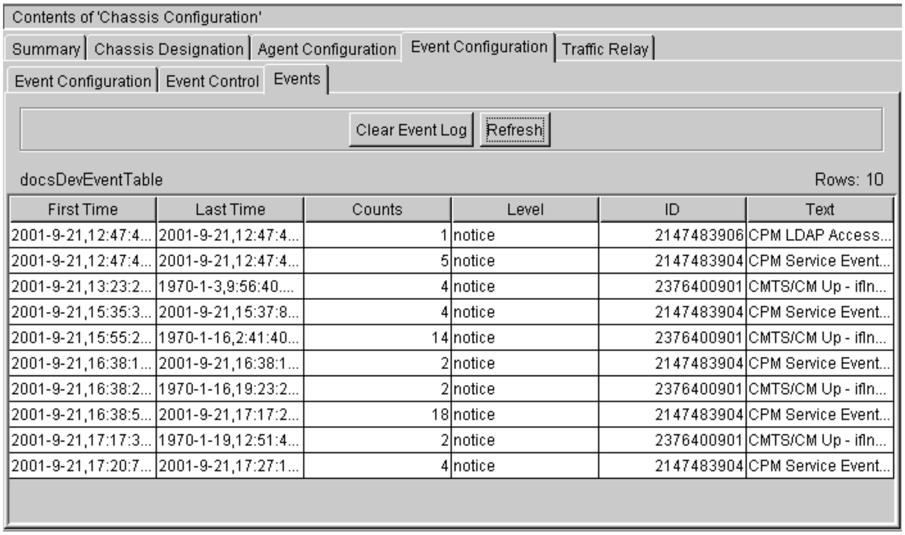
Viewing the Events

You can view the log of events that the Cuda has generated. To view the events follow this procedure:

1. In the Event Configuration window, click the **Events** tab. The docsDevEventTable window appears.
2. Click **Refresh** to update the information.

What you See

Figure 8-4 Log of Events



docsDevEventTable Rows: 10

First Time	Last Time	Counts	Level	ID	Text
2001-9-21,12:47:4...	2001-9-21,12:47:4...	1	notice	2147483906	CPM LDAP Access...
2001-9-21,12:47:4...	2001-9-21,12:47:4...	5	notice	2147483904	CPM Service Event...
2001-9-21,13:23:2...	1970-1-3,9:56:40....	4	notice	2376400901	CMTS/CM Up - ifIn...
2001-9-21,15:35:3...	2001-9-21,15:37:8...	4	notice	2147483904	CPM Service Event...
2001-9-21,15:55:2...	1970-1-16,2:41:40...	14	notice	2376400901	CMTS/CM Up - ifIn...
2001-9-21,16:38:1...	2001-9-21,16:38:1...	2	notice	2147483904	CPM Service Event...
2001-9-21,16:38:2...	1970-1-16,19:23:2...	2	notice	2376400901	CMTS/CM Up - ifIn...
2001-9-21,16:38:5...	2001-9-21,17:17:2...	18	notice	2147483904	CPM Service Event...
2001-9-21,17:17:3...	1970-1-19,12:51:4...	2	notice	2376400901	CMTS/CM Up - ifIn...
2001-9-21,17:20:7...	2001-9-21,17:27:1...	4	notice	2147483904	CPM Service Event...

Parameter Descriptions

This table provides a description of the log parameters:

Table 8-5 docsDevEvent Table Window

Field	Description
First Time	The time that the log entry was created.

Field	**Description**
Last Time	The time that the last event associated with the log entry occurred. In some cases, multiple events can be associated with a single log entry. This tends to happen when duplicate events are reported. However, when only one event is reported, then one event is associated with an entry, which means that the First Time and Last Time values are the same.
Counts	The number of consecutive event instances that this event entry reports. The count starts at 1 when the entry is created and increments by one for each subsequent duplicate event.
Level	The event’s class (emergency, alert, critical, error, warning, notice, info, debug).
ID	An internal event identifier.
Text	Brief description of the event associated with the ID.

Clearing the Event Log

To prevent your internal event log from consuming too much disk space, you may want to clear the log periodically. Use this procedure to clear the event log:

1. In the Event Configuration window, click the **Events** tab.
2. Click **Clear Event Log** to clear the log.
3. Click **Refresh** to update the information.

9 MODULE ADMINISTRATION

Cuda 12000 modules interface with cable and IP networks. This chapter describes the Cuda modules and explains how to manage the modules from within CudaView and includes:

- About Cuda 12000 Modules
- About Card Summary
- Viewing Module Topology
- Managing Modules
- Configuring the POS Clock Source
- Monitoring Buffer Pool Size
- Monitoring CPU Utilization
- Ethernet Interface Administration

This chapter assumes that you have already configured the chassis as provided in Chapter 5, “Chassis Management”.

NOTE: Administration of the Packet Over SONET (POS) module is explained in Chapter 10, “Packet Over SONET Administration”.

About Cuda 12000 Modules

The Cuda 12000 provides administrative status and other key information about the modules that are installed in the Cuda.

This table describes the module types that the Cuda supports for network administration and configuration:

Table 9-1 Modules Supported by the Cuda 12000

Module Type	Description
DOCSIS 1x4 SpectraFlow	Provides 1x4 CMTS functionality to provide cable modem connectivity and data passing over your domestic cable network. *(1x4 refers to a channel ratio of 1 downstream channel-to-4 upstream channels.)*
DOCSIS 1x6spm SpectraFlow	Provides CMTS functionality to provide cable modem connectivity and data passing over your domestic cable network at a channel ratio of 2 downstream channels-to-6 upstream channels. This module includes on board adaptive spectrum management circuitry and supports the Active-Active 1+1 HFC redundancy scheme to allow the operator the module to offer HFC module failure protection.
EuroDOCSIS 1x4 SpectraFlow	Provides 1x4 CMTS functionality to provide cable modem connectivity and data passing over your European cable network.*(1x4 refers to a channel ratio of 1 downstream channel-to-4 upstream channels.)*
EuroDOCSIS 1x4spm SpectraFlow	Provides CMTS functionality to provide cable modem connectivity and data passing over your European cable network at a channel ratio of 2 downstream channels-to-4 upstream channels. This module includes on board adaptive spectrum management circuitry and supports the Active-Active 1+1 HFC redundancy scheme to allow the operator the module to offer HFC module failure protection.
Octal 10/100 Ethernet SpectraFlow	Provides eight autosensing 10/100 Mbps ports for connection to your IP network. *The Ethernet module may be configured to function as a route server.*
Gigabit Ethernet SpectraFlow	Provides a 1 Gbps port for connection to your IP network.*The Gigabit module may be configured to function as a route server.*

Table 9-1 Modules Supported by the Cuda 12000 (continued)

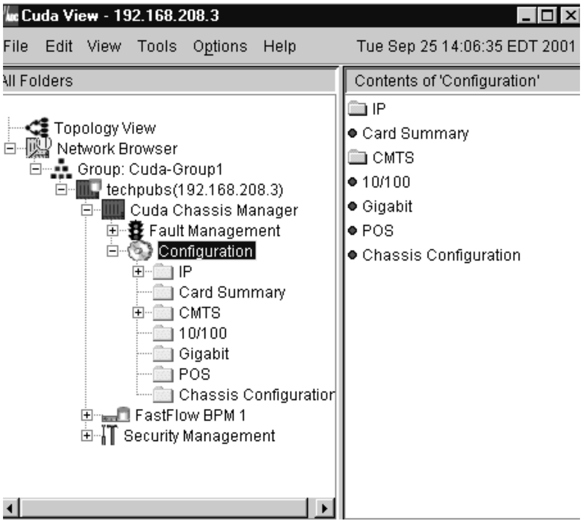
Module Type	Description
Packet Over SONET (POS) SpectraFlow	Enables the Cuda 12000 to transmit IP packets directly over SONET links, essentially, placing the IP layer directly over the SONET physical layer.

Module management is performed within the Configuration functional area in CudaView.

To access module administration, navigate to **Network Browser** > GroupName> ChassisName> **Cuda Chassis Manager**> **Configuration.** The Configuration folders appear.

What you see

Figure 9-1 Configuration Folder Display



About Card Summary

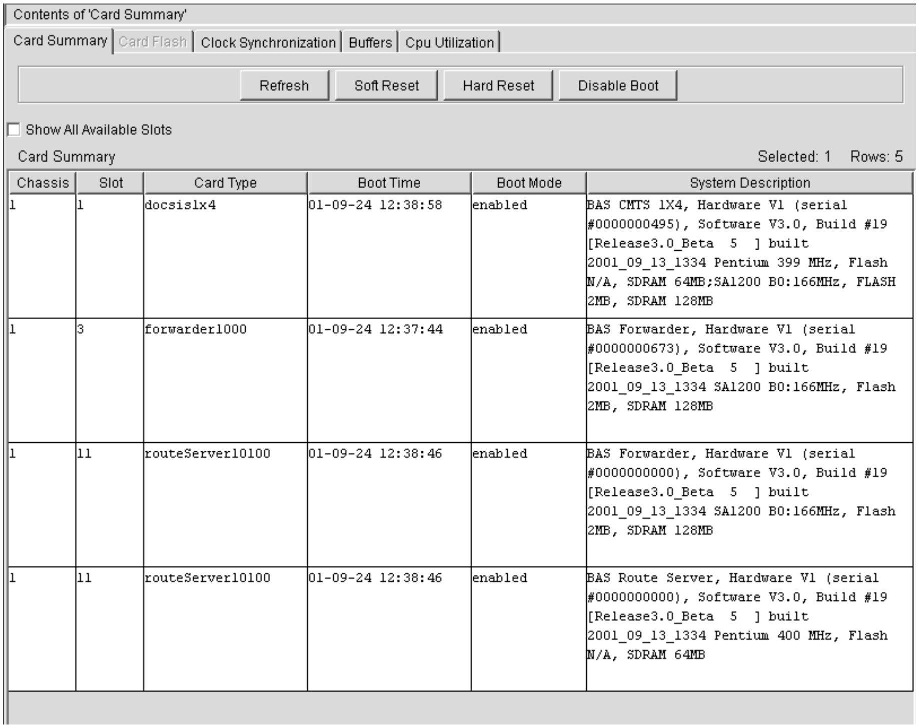
Card Summary provides an overview of the modules and allows you to manage modules that are installed on your Cuda 12000. Within Card Summary you can:

- View module topology
- Reset a selected module
- Disable a selected module
- View Clock Synchronization Status
- Monitor Buffer Size
- Monitor CPU Utilization

To access Card Summary, navigate to **Network Browser** > GroupName> ChassisName> **Cuda Chassis Manager** > **Configuration** > **Card Summary.**

What You See

Figure 9-2 Card Summary Window



□ Show All Available Slots

Card Summary

Selected: 1 Rows: 5

Chassis	Slot	Card Type	Boot Time	Boot Mode	System Description
1	1	docsis1x4	01-09-24 12:38:58	enabled	BAS CMTS 1X4, Hardware V1 (serial #0000000495), Software V3.0, Build #19 [Release3.0_Beta 5] built 2001_09_13_1334 Pentium 399 MHz, Flash N/A, SDRAM 64MB;SA1200 B0:166MHz, FLASH 2MB, SDRAM 128MB
1	3	forwarder1000	01-09-24 12:37:44	enabled	BAS Forwarder, Hardware V1 (serial #0000000673), Software V3.0, Build #19 [Release3.0_Beta 5] built 2001_09_13_1334 SA1200 B0:166MHz, Flash 2MB, SDRAM 128MB
1	11	routeServer10100	01-09-24 12:38:46	enabled	BAS Forwarder, Hardware V1 (serial #0000000000), Software V3.0, Build #19 [Release3.0_Beta 5] built 2001_09_13_1334 SA1200 B0:166MHz, Flash 2MB, SDRAM 128MB
1	11	routeServer10100	01-09-24 12:38:46	enabled	BAS Route Server, Hardware V1 (serial #0000000000), Software V3.0, Build #19 [Release3.0_Beta 5] built 2001_09_13_1334 Pentium 400 MHz, Flash N/A, SDRAM 64MB

Viewing Module Topology

You may view a summary of the current system topology. The topology information includes the following:

- A list of all installed modules
- The physical ports in which the modules are installed
- Module status
- Module software and hardware versions
- Module description

To view the summary information, follow this procedure:

1. Navigate to the Card Summary folder.
2. Click the **Card Summary** tab. The Card Summary window appears. (Refer to Figure 9-2.)
3. Click **Refresh** to update the information.

Parameter Descriptions

This table provides a description of the summary information available for installed modules.

Table 9-2 Card Summary Window Parameters

Parameter	Description
Chassis	Unique ID you assigned to the chassis
Slot	Number of the physical chassis slot in which the card resides. For information on how slots are numbered, see the "Cuda 12000 Installation Guide".
Card Type	The module type that is installed in the chassis.
Boot Time	Date and time that the interface came online and initialized with the management module.
Boot Mode	Indicates whether the module is enabled or disabled. Enabled indicates the module is active. Disabled indicates the module is not active.
System Description	Provides the following information about a module:

Parameter	Description
Functional Capacity	Functional capacity of the module, such as whether the module is a DOCSIS or EuroDOCSIS CMTS, or Ethernet, Gigabit or POS that may serve as a forwarder and/or route server.
Hardware Version	Version of module hardware.
Software Version	Version of software installed on the module.
Build Number	Assigned software build number.
Build Date	Time stamp indicating build date.

Managing Modules

You can reset and disable modules on your Cuda 12000, using the buttons within the Card Summary window.

Buttons

This table provides a description of the button functions, within the Card Summary window:

Table 9-3 Card Summary Buttons

Button	Description
Refresh	Updates the window with the current information.
Soft Reset	Resets the module by rebooting the module.
Hard Reset	Resets the module, but does not reboot the module.
Enable/Disable Boot	Sets the module to active or non active status. Enabled indicates active status. Disabled indicates not active status.

Resetting Modules

To reset modules, follow this procedure. (Refer to Table 9-3.):

1. Navigate to the Card Summary folder.
2. Click the **Card Summary** tab. The Card Summary window appears.
3. Click **Refresh** to update the information.
4. Select the row that includes the module that you want to reset.(Refer to Figure 9-2.)
5. To reset and reboot the module, click the **Soft Reset** button.
6. To reset the module, but not reboot, click the **Hard Reset** button.

Enabling/Disabling Modules

You can set the module status to active or not active by toggling the Enable/Disable Boot button; follow this procedure. (Refer to Table 9-3.):

1. Click the Card Summary folder.
2. Click the **Card Summary** tab. The Card Summary window appears.
3. Click **Refresh** to update the information.

4. Select the row that includes the module that you want to reset. (Refer to Figure 9-2.) Go to the Boot Mode column.
5. If the status in the Boot Mode column is Disabled, the module is not active. Click the Enable Boot button to set the module status to active.
6. If the status in the Boot Mode column is Enabled, the module is active. Click the Disable Boot button to set the module status to not active.

Configuring the POS Clock Source

The Cuda 12000 allows you to configure the POS module as the clock source for the primary clock (A) and secondary clock (B), which are contained on the backplane.

If you use a POS module as the clock source, make sure that the interface on the POS module has been configured to receive clocking from the other (remote) side of the POS link. Refer to Chapter 10, "Packet Over SONET Administration" for more information on configuring POS interfaces.

The following table describes the Card Drive Clock configuration parameters:

Table 9-4 Card Drive Clock Parameters

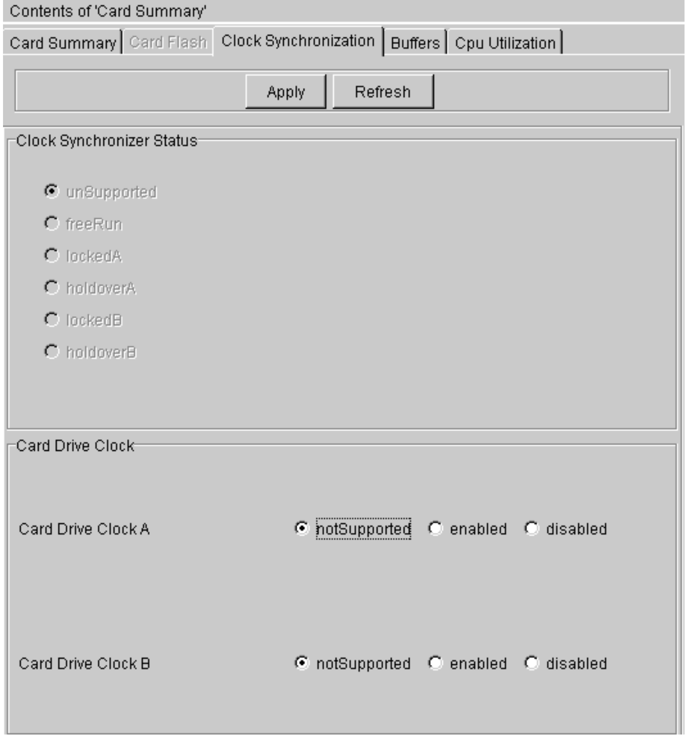
Parameter	Description
Card Drive Clock A	Refers to the primary clock (A) on the backplane. Configuration options are: ■ notSupported ■ Enabled ■ Disabled
Card Drive Clock B	Refers to the secondary clock (B) on the backplane. Configuration options are: ■ notSupported ■ Enabled ■ Disabled

To configure the POS module as the clock source, follow this procedure:

1. Navigate to the Card Summary folder.
2. Click the **Card Summary** tab. The Card Summary window appears. (Refer to Figure 9-2.)
3. Refer to the Card Type column to find the POS module, which is listed as forwarderOC3 or forwarderOC12.
4. Select the row that includes the POS module.
5. Click the **Clock Synchronization** tab. The Clock Synchronization window appears. (Refer to Figure 9-3.)

6. To configure the POS module as the clock source for the primary clock (A), choose Enabled for Card Drive Clock A.
7. To configure the POS module as the clock source for the secondary clock (B), choose Enabled for Card Drive Clock B.
8. Click **Apply** to commit the changes.

Figure 9-3 Clock Synchronization Window



Contents of 'Card Summary'

Clock Synchronizer Status

● unSupported
○ freeRun
○ lockedA
○ holdoverA
○ lockedB
○ holdoverB

Card Drive Clock

Card Drive Clock A ● notSupported ○ enabled ○ disabled

Card Drive Clock B ● notSupported ○ enabled ○ disabled

For more information about clock sources on the Cuda 12000, refer to Chapter 5, “Chassis Management”. For more information about clock connectors on the Cuda 12000, refer to the *Cuda 12000 IP Access Switch Installation Guide*.

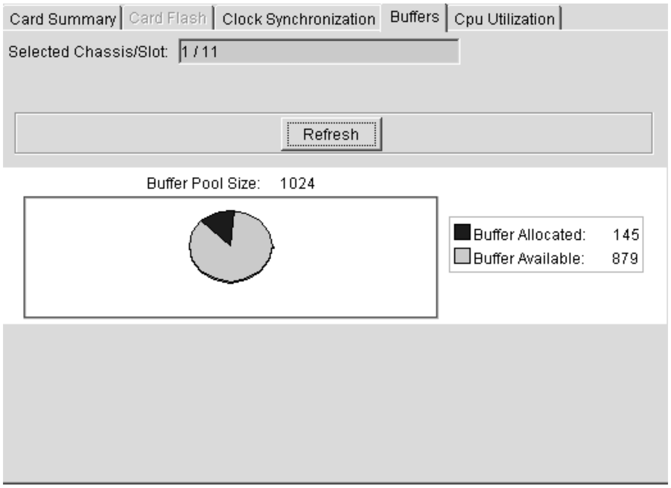
Monitoring Buffer Pool Size

You may monitor buffer usage for all application modules, except the management module. Buffer usage is displayed by a pie graph. To access the Buffer Pool Size pie graph, follow this procedure:

1. Navigate to the Card Summary folder.
2. Click the **Card Summary** tab. The Card Summary window appears.
3. Click **Refresh** to update the information.
4. Select the row that includes the module that you want to monitor. (Refer to Figure 9-2.)
5. Click the **Buffers** tab. The Buffer Pool Size pie graph appears.
6. Monitor buffer usage. Refer to Table 9-5.

What you see

Figure 9-4 Buffer Pool Size Pie Graph



Selected Chassis/Slot: 1 / 11

Buffer Pool Size: 1024

■ Buffer Allocated: 145
□ Buffer Available: 879

Parameter Description

This table describes the buffer pool size pie graph parameters.

Table 9-5 Buffer Pool Size Parameters

Parameter	Description
Buffer Pool Size	The total number of memory buffers for the module. The total equals the sum of the allocated buffers and available buffers.
Buffer Allocated	The total number of memory allocated memory buffers.
Buffer Available	The total number of available (free) memory buffers.

Monitoring CPU Utilization

You may monitor CPU utilization for both the network processor and Pentium processor on installed modules. All forwarding modules utilize a network processor. Only DOCSIS/EuroDOCSIS modules and route server modules utilize the additional Pentium processor.

CPU utilization may be monitored for the following duration:

- 1 minute
- 1 hour
- 1 day

Viewing CPU Utilization

Following are characteristics of the CPU utilization viewing options:

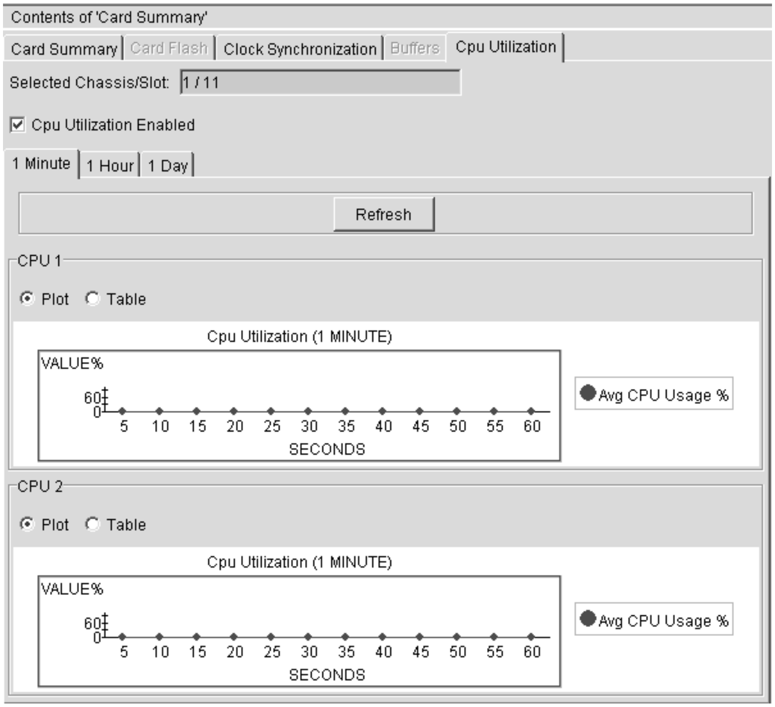
- A view is displayed for the network processor, and a view is displayed for the Pentium processor.
- Utilization is displayed by a plot graph view or a table view.

To view CPU utilization, follow this procedure:

1. Navigate to the Card Summary folder.
2. Click the **Card Summary** tab. The Card Summary window appears.
3. Click **Refresh** to update the information.
4. Select the row that includes the module that you want to view. (Refer to Figure 9-2.)
5. Click the **Cpu Utilization** tab. The Cpu Utilization window appears, and is displayed in the plot or table view. (Refer to Figure 9-5 and Figure 9-6.)
6. To monitor CPU utilization, choose the Enable Cpu Utilization Enabled option.
7. Click the tab for the duration of time you want to monitor utilization.
8. Choose the Plot or Table option for the display you want to view.
9. View CPU utilization. (Refer to Table 9-5.)

What You See

Figure 9-5 CPU Utilization Plot Graph Window



Contents of 'Card Summary'

Selected Chassis/Slot: 1 / 11

☑ Cpu Utilization Enabled

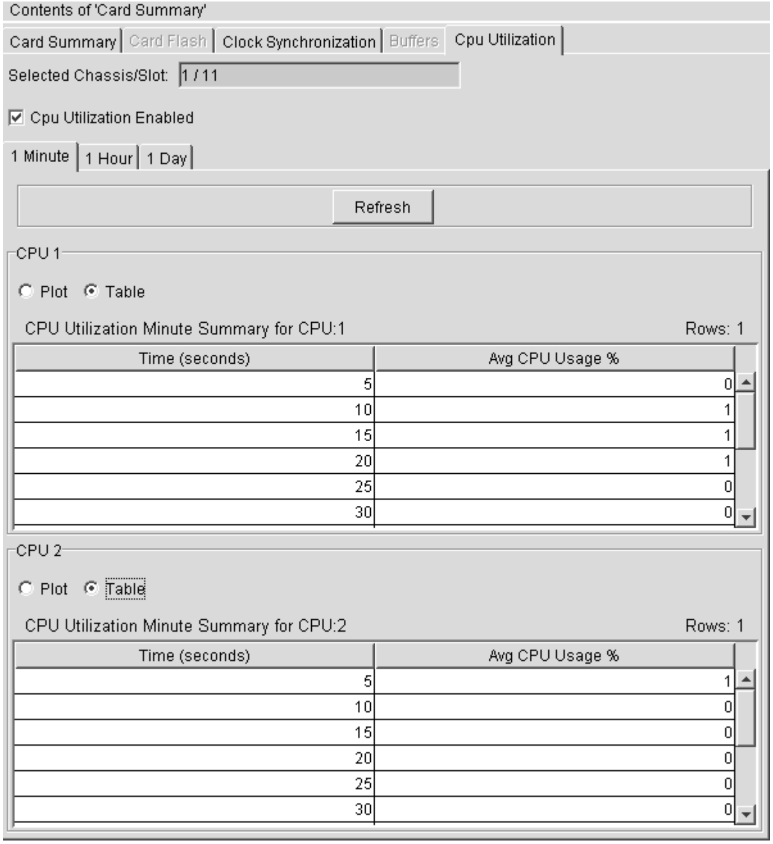
CPU 1

● Plot ○ Table

CPU 2

● Plot ○ Table

Figure 9-6 CPU Utilization Table Window



Contents of 'Card Summary'

Selected Chassis/Slot: 1 / 11

☑ Cpu Utilization Enabled

CPU 1

○ Plot ● Table

CPU Utilization Minute Summary for CPU:1 Rows: 1

Time (seconds)	Avg CPU Usage %
5	0
10	1
15	1
20	1
25	0
30	0

CPU 2

○ Plot ● Table

CPU Utilization Minute Summary for CPU:2 Rows: 1

Time (seconds)	Avg CPU Usage %
5	1
10	0
15	0
20	0
25	0
30	0

Parameter Descriptions

This table describes the Cpu Utilization window parameters.

Table 9-6 Cpu Utilization Parameters

Parameter	Description
CPU 1	Displays CPU utilization for the network processor. This is applicable to all forwarding modules.
CPU 2	Displays CPU utilization for the on-board Pentium processor. This is applicable only to DOCSIS/EuroDOCSIS modules, and modules configured as the route server.
Usage%	Indicates the percentage of CPU usage and the percentage of time in which utilization is monitored.

Parameter	Description
Time	Indicates the duration of time in which CPU utilization is monitored. The options are: ■ 1 minute in 5 second intervals ■ 1 hour in 1 minute intervals ■ 1 day in 1 hour intervals

Ethernet Interface Administration

Ethernet, also known as IEEE 802.3, uses a “Carrier Sense, Multiple Access, Collision Detect (CSMA/CD)” protocol to control multiple stations accessing one cable. The functions of Ethernet are:

- Transmitting and receiving packets
- Validating addresses
- Detecting packet errors

The Cuda 12000 supports two Ethernet interfaces, which are:

- Octal 10/100 Ethernet — Provides eight autosensing 10/100 Mbps ports for connection to your IP network
- Gigabit Ethernet. — Provides a 1 Gbps port for connection to your IP network.

The Cuda 12000 allows the Ethernet modules to function as a route server. A module is configured as a route server at the ADC plant before the Cuda is shipped.

This section describes Ethernet interface administration and includes the following topics for the 10/100 and Gigabit Ethernet interfaces:

- Managing the 10/100 Ethernet Interface
- Managing the Gigabit Ethernet Interface

Managing the 10/100 Ethernet Interface

Managing the 10/100 Ethernet interface includes:

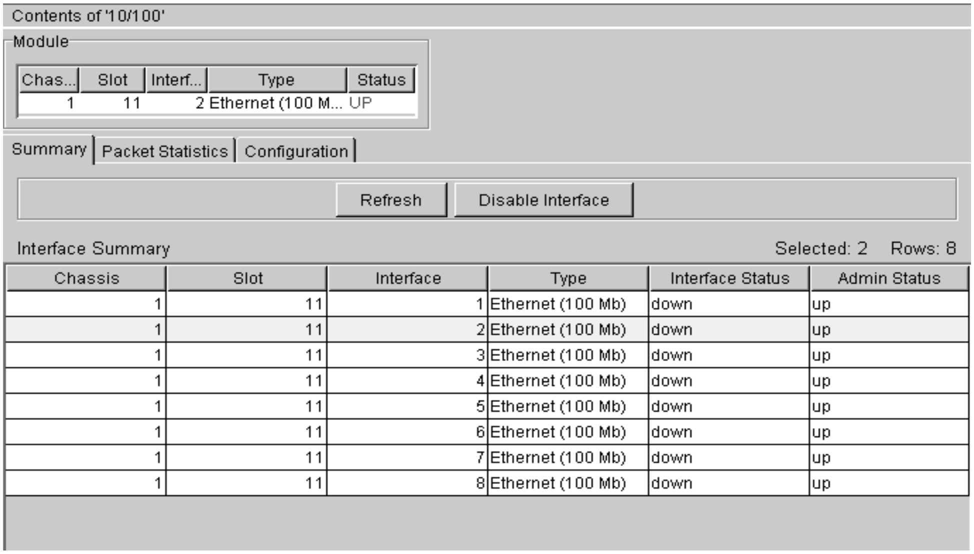
- Viewing 10/100 Ethernet Interfaces
- Disabling and Enabling 10/100 Interfaces
- Viewing 10/100 Ethernet Packet Statistics
- Configuring 10/100 Ethernet Duplex Mode and Speed

The 10/100 Ethernet interface is managed within the 10/100 folder. To access the 10/100 folder, follow this procedure:

1. Navigate to Configuration.
2. Click the10/100 folder. The 10/100 window is displayed.

What You See

Figure 9-7 10/100 Interface Summary window.



Chas...	Slot	Interf...	Type	Status
1	11	2	Ethernet (100 M...	UP

Interface Summary Selected: 2 Rows: 8

Chassis	Slot	Interface	Type	Interface Status	Admin Status
1	11	1	Ethernet (100 Mb)	down	up
1	11	2	Ethernet (100 Mb)	down	up
1	11	3	Ethernet (100 Mb)	down	up
1	11	4	Ethernet (100 Mb)	down	up
1	11	5	Ethernet (100 Mb)	down	up
1	11	6	Ethernet (100 Mb)	down	up
1	11	7	Ethernet (100 Mb)	down	up
1	11	8	Ethernet (100 Mb)	down	up

About the 10/100 Ethernet Window

The window is divided into two panels: The Module and the Tabs.

Module Panel

The Module panel is a context-sensitive heading panel that displays the following information for the selected interface:

Table 9-7 10/100 Module Panel Parameters

Parameter	Description
Chassis	Unique ID you assigned to the chassis
Slot	Number of the physical chassis slot in which the card resides. For information on how slots are numbered, see the *Cuda 12000 IP Access Switch Installation Guide*.
Interface	Number of this physical interface on the module.
Type	Indicates the type of Ethernet link.
Status	Online status of this physical interface. Indicates whether the module is UP (online) or DOWN (offline).

The Tab Panel

The Tab panel includes the following module management tabs, which are described in the appropriate sections below:

- Summary
- Packet Statistics
- Configuration

Viewing 10/100 Ethernet Interfaces

You may view summary information for all the 10/100 interfaces installed on your Cuda 12000.

To view summary information, follow this procedure:

1. Navigate to the 10/100 folder.
2. Click the **Summary** tab. The Interface Summary window appears. (Refer to Figure 9-7.)

Interface Summary Window

The Interface Summary window displays all the 10/100 interfaces installed on the Cuda 12000.

This table describes the 10/100 Interface Summary window parameters.

Table 9-8 10/100 Module Summary Window Parameters

Parameter	Description
Chassis	Unique ID you assigned to the chassis
Slot	Number of the physical chassis slot in which the card resides. For information on how slots are numbered, see the *Cuda 12000 IP Access Switch Installation Guide*.
Interface	Number of this physical interface on the module.
Type	Indicates the type of Ethernet link.
Interface Status	Indicates that you have a valid link (connection) on that interface. Up indicates a valid link is established; down indicates there is no link on that interface.
Admin Status	Online status of this physical interface. Indicates whether the module is up (online) or down (offline).

Disabling and Enabling 10/100 Interfaces

You can manually take a physical interface offline or bring it online.

To disable an interface follow this procedure:

1. Navigate to the 10/100 folder.
2. Click the **Summary** tab. The Interface Summary window appears. (Refer to Figure 9-7.)
3. Select the row that includes the interface that you want to bring offline.

To take an interface offline:

4. Click **Disable Interface**. When you disable the interface, the Admin Status indicates that the interface is down. The interface can no longer forward traffic.
5. Click **Refresh** to update the information.

To bring an interface online:

6. Repeat steps 1 through 3 above.
7. Click **Enable Interface**. When you enable the interface, the Administration Status indicates that the interface is up. The interface is able to forward traffic.
8. Click **Refresh** to update the information.

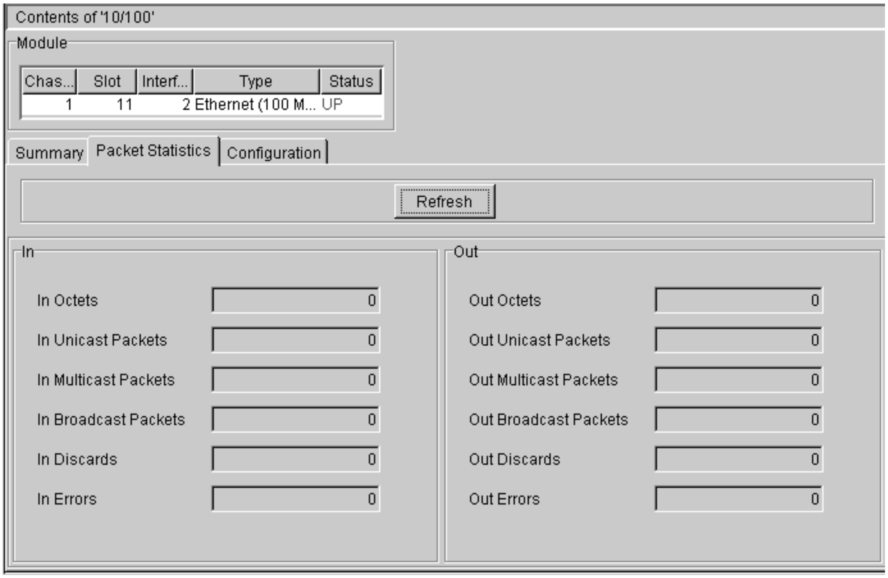
Viewing 10/100 Ethernet Packet Statistics

You can view both incoming packet statistics and outgoing packet statistics for a selected 10/100 Ethernet interface. To view packet statistics follow this procedure:

1. Navigate to the 10/100 folder.
2. Click the **Summary** tab. The Interface Summary window appears. (Refer to Figure 9-7.).
3. Select the row that includes the interface that you want to view.
4. Click the **Packet Statistics** tab.
5. Click **Refresh** to update the information.

What You See

Figure 9-8 10/100 Interface Packet Statistics window.



Chas...	Slot	Interf...	Type	Status
1	11	2	Ethernet (100 M...	UP

In Octets	0
In Unicast Packets	0
In Multicast Packets	0
In Broadcast Packets	0
In Discards	0
In Errors	0

Out Octets	0
Out Unicast Packets	0
Out Multicast Packets	0
Out Broadcast Packets	0
Out Discards	0
Out Errors	0

Parameter Descriptions

This table provides a description of the 10/100 Packet Statistics window.

Table 9-9 10/100 Packet Statistics Parameters

Parameter	Description
In	
In Octets	Total number of Octets that have been received on this interface, including framing characters.
In Unicast Packets	Number of Unicast packets that have been received on this interface.
In Multicast Packets	Number of Multicast packets that have been received on this interface.
In Broadcast Packets	Number of Broadcast packets that have been received on this interface.
In Discards	Received FIFO overflows.
In Errors	Number of error packets received on this interface.
Out	
Out Octets	Total number of octets that have been transmitted from this interface, including framing characters.
Out Unicast Packets	Total number of Unicast packets that have been transmitted from this interface.
Out Multicast Packets	Total number of Multicast packets that have been transmitted from this interface.
Out Broadcast Packets	Total number of Broadcast packets that have been transmitted from this interface.
Out Discards	Transmitted FIFO underflows.
Out Errors	Total number of error packets transmitted from this interface.

Configuring 10/100 Ethernet Duplex Mode and Speed

The Cuda 12000 allows you to configure duplex mode and speed on the 10/100 module.

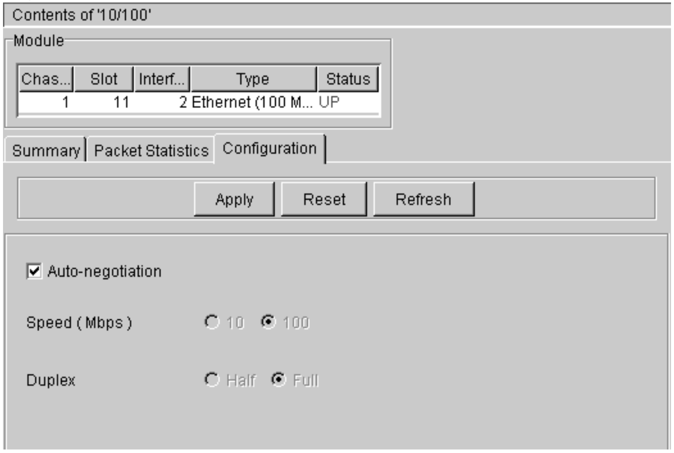
You may set duplex mode to full duplex, half duplex, or auto negotiation. You may set the speed to 10 Mpbs, 100 Mbps, or auto negotiation. By default, the Cuda 12000 sets duplex mode and speed to auto negotiation.

To configure duplex mode and speed on the 10/100 module, follow this procedure:

1. Navigate to the 10/100 folder.
2. Click the **Summary** tab. The Interface Summary window appears. (Refer to Figure 9-7.).
3. Select the row that includes the module that you want to configure.
4. Click the **Configuration** tab. The Configuration window appears.
5. Disable Auto-negotiation. *If Auto-negotiation is enabled, a check-mark appears in the Auto-negotiation field.*
6. Select the speed and duplex mode that you want to configure for the specific module. (Refer to Table 9-10.)
7. Click **Apply** to commit the changes;, or click **Reset** to return to the original configuration.

What You See

Figure 9-9 10/100 Configuration Window



Contents of '10/100'

Module

Chas...	Slot	Interf...	Type	Status
1	11	2	Ethernet (100 M...	UP

☑ Auto-negotiation

Speed (Mbps) ○ 10 ● 100

Duplex ○ Half ● Full

Parameter Descriptions

This table describes the 10/100 configuration parameters:

Table 9-10 10/100 Configuration Parameters

Parameter	Description
Auto-negotiation	Configures the 10/100 Ethernet port to automatically negotiate duplex mode and speed. By default, the Cuda 12000 is set to auto-negotiation.
Speed (Mpbs)	Sets the speed on the 10/100 Ethernet port. The options are: ■ 10 Mbps - Sets the speed to 10 Mbps. ■ 100 Mbps. - Sets the speed to 100 Mbps. Note: If you configure the port for 10 Mbps or 100 Mbps, you also set the duplex mode to its last explicit setting (half or full).

Parameter	**Description**
Duplex	Sets the duplex mode on the 10/100 Ethernet port. The options are: ■ Full - Sets the port to full-duplex mode (port can send and receive simultaneously). Note that, if you configure the port for full duplex or half duplex, you also set the speed to its last explicit setting (100 or 100). ■ Half - Sets the port to half-duplex mode (port cannot sent and receive simultaneously).

Managing the Gigabit Ethernet Interface

Managing the Gigabit Ethernet interface includes:

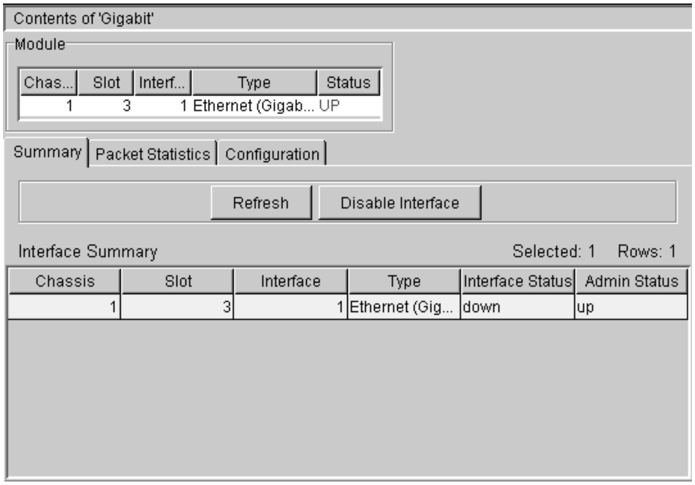
- Viewing Gigabit Ethernet Interfaces
- Disabling and Enabling Gigabit Interfaces
- Viewing Gigabit Ethernet Packet Statistics
- Configuring Gigabit Ethernet Duplex Mode

The Gigabit Ethernet interface is managed within the Gigabit folder. To access the Gigabit folder, follow this procedure:

1. Navigate to Configuration.
2. Click the Gigabit folder. The Gigabit window appears.

What You See

Figure 9-10 Gigabit window



Contents of 'Gigabit'

Module

Chas...	Slot	Interf...	Type	Status
1	3	1	Ethernet (Gigab...	UP

Interface Summary Selected: 1 Rows: 1

Chassis	Slot	Interface	Type	Interface Status	Admin Status
1	3	1	Ethernet (Gig...	down	up

About the Gigabit Ethernet Window

The window is divided into two panels: The Module and the Tabs.

Module Panel

The Module panel is a context-sensitive heading panel that displays the following information for the selected interface:

Table 9-11 Gigabit Module Panel Parameters

Parameter	Description
Chassis	Unique ID you assigned to the chassis
Slot	Number of the physical chassis slot in which the module resides. For information on how slots are numbered, see the *Cuda 12000 IP Access Switch Installation Guide*.
Interface	Number of this physical interface on the module.
Type	Indicates the type of Ethernet link.
Status	Online status of this physical interface. Indicates whether the module is UP (online) or DOWN (offline).

The Tab Panel

The Tab panel includes the following module management tabs, which are described in the appropriate sections below:

- Summary
- Packet Statistics
- Configuration

Viewing Gigabit Ethernet Interfaces

You may view summary information for all the Gigabit interfaces installed on your Cuda 12000.

To view summary information, follow this procedure:

1. Navigate to the Gigabit folder.
2. Click the **Summary** tab. The Interface Summary window appears. (Refer to Figure 9-10.)

Interface Summary Window

The Interface Summary window displays all the Gigabit interfaces installed on the Cuda 12000.

This table describes the Gigabit Interface Summary window parameters.

Table 9-12 Gigabit Module Summary Window Parameters

Parameter	Description
Chassis	Unique ID you assigned to the chassis
Slot	Number of the physical chassis slot in which the module resides. For information on how slots are numbered, see the *Cuda 12000 IP Access Switch Installation Guide*.
Interface	Number of this physical interface on the module.
Type	Indicates the type of Ethernet link.
Interface Status	Indicates that you have a valid link (connection) on that interface. Up indicates a valid link is established; down indicates there is no link on that interface.
Admin Status	Online status of this physical interface. Indicates whether the module is up (online) or down (offline).

Disabling and Enabling Gigabit Interfaces

You can manually take a physical interface offline or bring it online.

To disable an interface follow this procedure:

1. Navigate to the Gigabit folder.
2. Click the **Summary** tab. The Interface Summary window appears. (Refer to Figure 9-10.)
3. Select the row that includes the interface that you want to bring offline.

To take an interface offline:

4. Click **Disable Interface**. When you disable the interface, the Admin Status indicates that the interface is down. The interface can no longer forward traffic.
5. Click **Refresh** to update the information.

To bring an interface online:

1. Repeat steps 1 through 3 above.
2. Click **Enable Interface**. When you enable the interface, the Administration Status indicates that the interface is up. The interface is able to forward traffic.
3. Click **Refresh** to update the information.

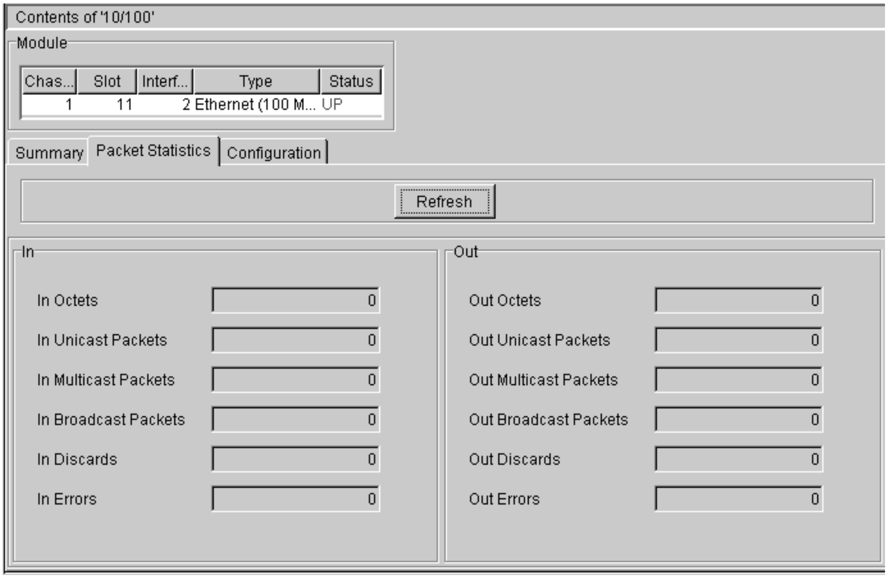
Viewing Gigabit Ethernet Packet Statistics

You can view both incoming packet statistics and outgoing packet statistics for a selected Gigabit Ethernet interface. To view packet statistics follow this procedure:

1. Navigate to the Gigabit folder.
2. Click the **Summary** tab. The Interface Summary window appears. (Refer to Figure 9-10.).
3. Select the row that includes the interface that you want to view.
4. Click the **Packet Statistics** tab. The Packet Statistics window appears.
5. Click **Refresh** to update the information.

What You See

Figure 9-11 Gigabit Interface Packet Statistics window.



Contents of '10/100'

Module

Chas...	Slot	Interf...	Type	Status
1	11	2	Ethernet (100 M...	UP

In

In Octets	0
In Unicast Packets	0
In Multicast Packets	0
In Broadcast Packets	0
In Discards	0
In Errors	0

Out

Out Octets	0
Out Unicast Packets	0
Out Multicast Packets	0
Out Broadcast Packets	0
Out Discards	0
Out Errors	0

Parameter Descriptions

This table provides a description of the Gigabit Packet Statistics window.

Table 9-13 Gigabit Packet Statistics Parameters

Parameter	Description
In	
In Octets	Total number of Octets that have been received on this interface, including framing characters.
In Unicast Packets	Number of Unicast packets that have been received on this interface.
In Multicast Packets	Number of Multicast packets that have been received on this interface.
In Broadcast Packets	Number of Broadcast packets that have been received on this interface.
In Discards	Received FIFO overflows.
In Errors	Number of error packets received on this interface.
Out	
Out Octets	Total number of octets that have been transmitted from this interface, including framing characters.
Out Unicast Packets	Total number of Unicast packets that have been transmitted from this interface.
Out Multicast Packets	Total number of Multicast packets that have been transmitted from this interface.
Out Broadcast Packets	Total number of Broadcast packets that have been transmitted from this interface.
Out Discards	Transmitted FIFO underflows.
Out Errors	Total number of error packets transmitted from this interface.

Configuring Gigabit Ethernet Duplex Mode

The Cuda 12000 allows you to configure duplex mode on the Gigabit module.

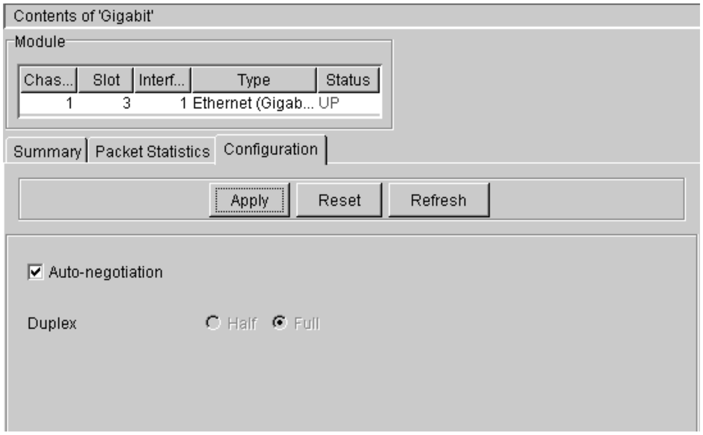
You may set duplex mode to full duplex, half duplex, or auto negotiation. By default, the Cuda 12000 sets duplex mode to auto negotiation.

To configure duplex mode on the Gigabit module, follow this procedure:

1. Navigate to the Gigabit folder.
2. Click the **Summary** tab. The Interface Summary window appears. (Refer to Figure 9-10.).
3. Select the row that includes the module that you want to configure.
4. Click the **Configuration** tab. The Configuration window appears.
5. Disable Auto-negotiation. *If Auto-negotiation is enabled, a check-mark appears in the Auto-negotiation field.*
6. Select the duplex mode that you want to configure for the specific module. (Refer to Table 9-14.)
7. Click **Apply** to commit the changes;, or click **Reset** to return to the original configuration.

What You See

Figure 9-12 Gigabit Configuration Window



Contents of 'Gigabit'

Module

Chas...	Slot	Interf...	Type	Status
1	3	1	Ethernet (Gigab...	UP

☑ Auto-negotiation

Duplex ○ Half ● Full

Parameter Descriptions

This table describes the Gigabit configuration parameters:

Table 9-14 Gigabit Configuration Parameters

Parameter	Description
Auto-negotiation	Configures the 10/100 Ethernet port to automatically negotiate duplex mode and speed. By default, the Cuda 12000 is set to auto-negotiation.
Duplex	Sets the duplex mode on the 10/100 Ethernet port. The options are: ▪ Full - Sets the port to full-duplex mode (port can send and receive simultaneously). Note that, if you configure the port for full duplex or half duplex, you also set the speed to its last explicit setting (100 or 100). ▪ Half - Sets the port to half-duplex mode (port cannot sent and receive simultaneously).

10 PACKET OVER SONET ADMINISTRATION

This section provides instruction on how to configure Packet over SONET (POS) on the Cuda 12000 using Cuda Chassis Manager and includes:

- About Packet Over SONET
- Packet Over SONET (POS) Interface Administration
- Configuring Point-to-Point Protocol (PPP)

The Cuda 12000 supports OC-3c and OC-12c SONET interfaces. For more information about OC-3c and OC-12c modules, refer to the "Cuda 12000 Installation Guide."

About Packet Over SONET

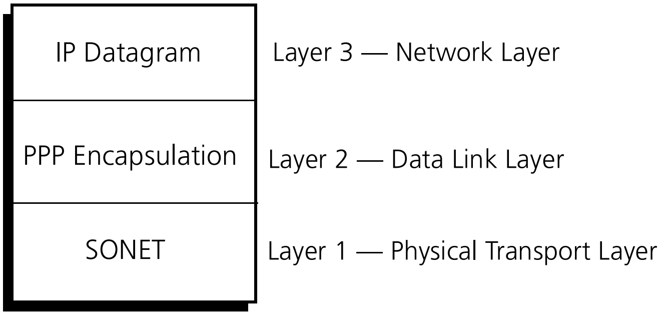
Packet Over SONET enables the Cuda 12000 to transmit IP packets over SONET links; essentially placing the IP layer over the SONET physical layer. POS makes efficient use of bandwidth, allowing for lower packet overhead and extremely fast transmission speeds.

The system uses point-to-point protocol (PPP) to transport IP data over SONET point-to-point circuits, as described in RFC 2615. The IP over SONET transmission process consists of three primary steps:

- Encapsulate the IP datagram into a PPP frame.
- Place the PPP frame into the payload portion of the SONET frame.
- Transmit the SONET frame over the point-to-point circuit.

Figure 10-1 shows the POS transport structure in relation to the OSI network model:

Figure 10-1 Packet Over SONET — Network Structure



POS administration on the Cuda 12000 involves:

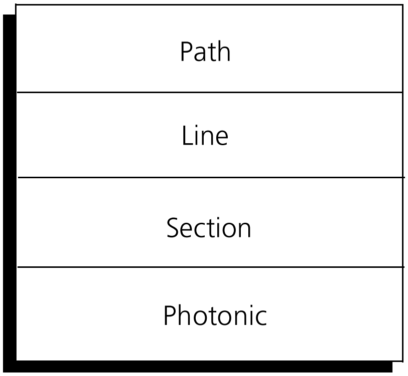
- Administration of the physical SONET interface at layer 1, as described in “Packet Over SONET (POS) Interface Administration,” next.
- Administration of the point-to-point protocol (PPP) used to encapsulate the IP data at layer 2, as described in “Configuring Point-to-Point Protocol (PPP)” on page 250.

Packet Over SONET (POS) Interface Administration

Packet over Synchronous Optical Network (SONET) allows for high-speed transport of IP data packets over a SONET STS network. The POS module contains a single physical interface that supports connection to STS networks and supports transmission speeds of up to 155 Mbps.

A SONET frame is 810 bytes represented as a grid of 9 rows by 90 columns. The frame consists of hierarchal layers, each providing services for the layer above it. Figure 10-2 shows the logical representation of the SONET layers.

Figure 10-2 SONET Network Structure



The layers that comprise a SONET frame include:

- **Path Layer** — Maps the payload into the synchronous payload envelope (SPE) of the SONET frame and creates the STS-1 synchronous payload envelope (SPE). In POS transmission, the payload contained in the SPE is the PPP encapsulated IP datagram. It then passes the resulting STS-1 SPE to the Line layer.
- **Line Layer** — Combines 3 STS-1 SPEs and adds the appropriate line overhead. This multiplexing of 3 STS-1 SPEs is also referred to as concatenation. It then passes the concatenated SPE to the section layer.
- **Section Layer** — Adds section overhead, performs scrambling, and creates the actual STS-3c and STS-12c frames, which it then passes to the photonic layer.
- Photonic Layer — Converts the electrical STS signals to an optical signal, referred to as Optical Carrier (OC). This OC signal is then transmitted over the circuit.

Each layer consists of its own overhead bytes. This overhead provides the powerful management and fault-tolerance capabilities inherent in a SONET network.

SONET overhead also provides for various alarms and error messages—known as defects—to be reported. Alarms allow for the reporting of network failures; error messages report incomplete failures that may compromise data transmission.

SONET interface administration on the Cuda 12000 includes:

- Viewing SONET Interface Information
- Disabling and Enabling Interfaces
- Viewing Interface Packet Statistics
- Viewing SONET Line Layer Statistics
- Viewing SONET Path Layer Information
- Viewing and Configuring Section Layer Administration
- Configuring and Viewing SONET Alarms

Before You Begin

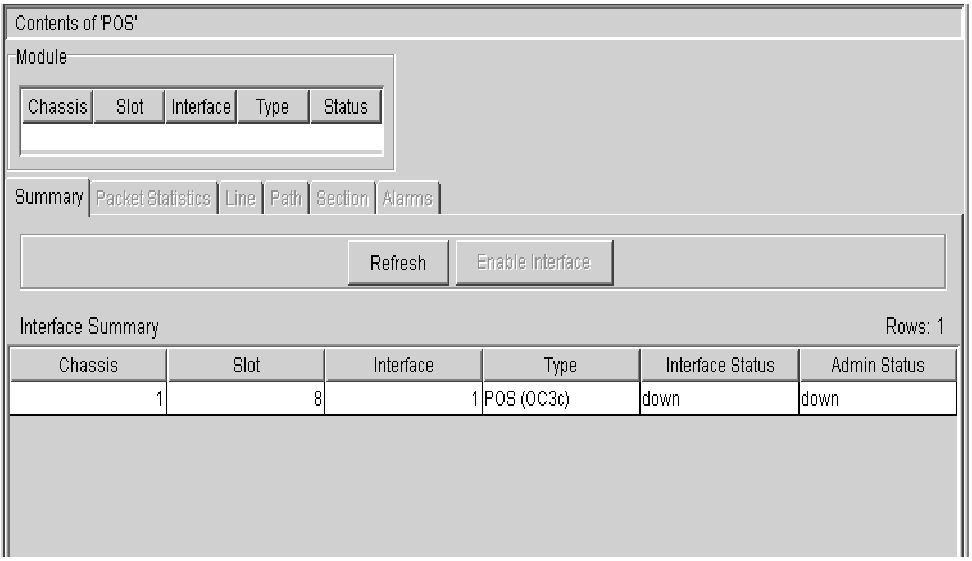
Located within the POS folder, the Summary display provides an at-a-glance listing of all POS interfaces installed in the system. The number of POS interfaces displayed is directly equivalent to the number of POS modules that you have installed, as each module has a single OC- STS interface.

To view the POS interface summary information, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **POS.**
2. Click the **Summary** tab.
3. Click **Refresh** to update the information.

What You See

Figure 10-3 POS Summary window.



Chassis	Slot	Interface	Type	Status

Chassis	Slot	Interface	Type	Interface Status	Admin Status
1	8	1	POS (OC3c)	down	down

Parameter Descriptions

This table provides a description of the POS Summary window

Table 10-1 .POS Summary Window Parameters

Parameter	Description
Chassis	ID of the chassis on which this interface resides.
Slot	Slot within the specified chassis on which this interface resides.
Interface	Number of this physical interface on the module *(always 1, as each POS module has a single interface)*.
Type	Type of POS interface. The system currently supports OC-3c and OC-12c interfaces.
Interface Status	Online status of this physical interface. Indicates whether the PPP connection is up or down.

Parameter	Description
Admin Status	Administrative status of this interface. When the Administrative status is up, the interface is online and can forward traffic over the PPP connection; when the administrative status is down, it cannot. You can manually set the administrative status of an interface. See “Disabling and Enabling Interfaces, ” next for details.

Disabling and Enabling Interfaces

You can manually change the administrative status of an interface. When an interface is enabled *(online)* it can forward traffic; when disabled *(offline)* it cannot.

Before you can change the administrative status of an interface, you must first select the interface. The button at the top of the summary display toggles between “Enable Interface” and “Disable Interface,” depending on the current administrative status of the selected interface.

To disable a POS interface, follow this procedure:

1. In the Summary window, select the interface that you want to bring offline.
2. Click on **Disable Interface.** Disabling the interface brings the PPP connection down and sets the administrative status to down. In this state, the interface cannot forward traffic.

To bring an interface online:

1. In the Summary window, select the interface that you want to bring online.
2. Select the interface that you want to bring online and click on **Enable Interface**. Enabling the interface starts PPP negotiations and sets the administrative status to up. When PPP negotiations complete, the interface can forward traffic.

NOTE*: This assumes that you have already configured a POS interface. For information about configuring POS interfaces, refer to the configuration sections beginning on page 246.*

Viewing Interface Packet Statistics

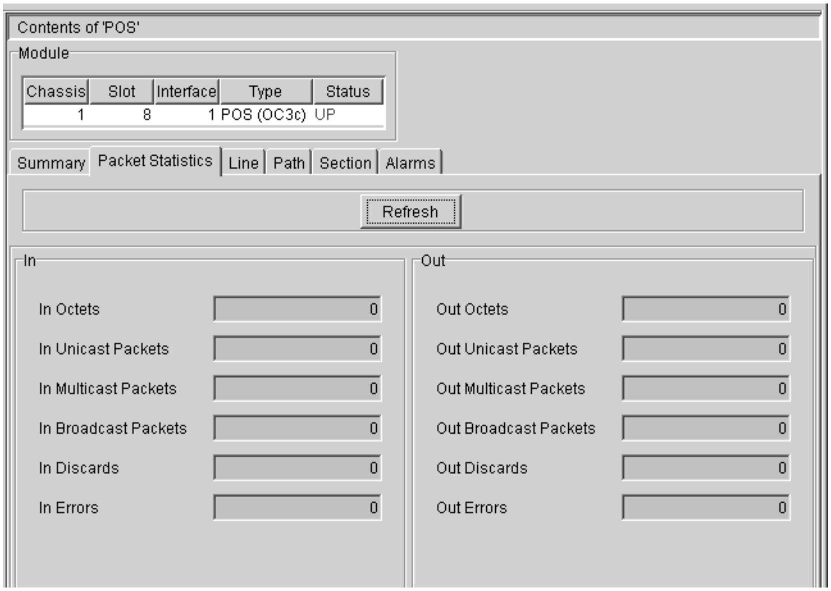
You can view both incoming and outgoing packet statistics for a selected POS interface. These traffic statistics provide a snapshot overview as to the amount and type of traffic flowing across the interface.

To view the interface packet statistics, follow this procedure:

1. In the Summary window, select the chassis that includes the interface you wish to view.
2. Click on the **Packet Statistics** tab.
3. Click **Refresh** to update the information.

What You See

Figure 10-4 This figure shows an example of the POS Packet Statistics window.



Chassis	Slot	Interface	Type	Status
1	8	1	POS (OC3c)	UP

In Octets: 0
In Unicast Packets: 0
In Multicast Packets: 0
In Broadcast Packets: 0
In Discards: 0
In Errors: 0

Out Octets: 0
Out Unicast Packets: 0
Out Multicast Packets: 0
Out Broadcast Packets: 0
Out Discards: 0
Out Errors: 0

Parameter Descriptions

This table provides a description of POS Packet Statistics window parameters.

Table 10-2 Summary Window

Parameter	Description
In	
In Octets	Total number of PPP negotiation octets that have been received on this interface. *This does not include octets for data packets.*
In Unicast Packets	Number of Unicast packets that have been received on this interface.
In Multicast Packets	Number of Multicast packets that have been received on this interface. *Currently not supported.*
In Broadcast Packets	Number of Broadcast packets that have been received on this interface. *Currently not supported.*
In Errors	Number of error packets received on this interface.
Out	
Out Octets	Total number of PPP negotiation octets that have been transmitted from this interface.
Out Unicast Packets	Total number of Unicast packets that have been transmitted from this interface.
Out Multicast Packets	Total number of Multicast packets that have been transmitted from this interface. *Currently not supported.*
Out Broadcast Packets	Total number of Broadcast packets that have been transmitted from this interface.*Currently not supported.*
Out Errors	Total number of error packets transmitted from this interface.

Viewing SONET Line Layer Statistics

The SONET Line layer serves as the path between multiplexers and is responsible for synchronizing data transmission and multiplexing the STS-1 signals generated by the section layer.

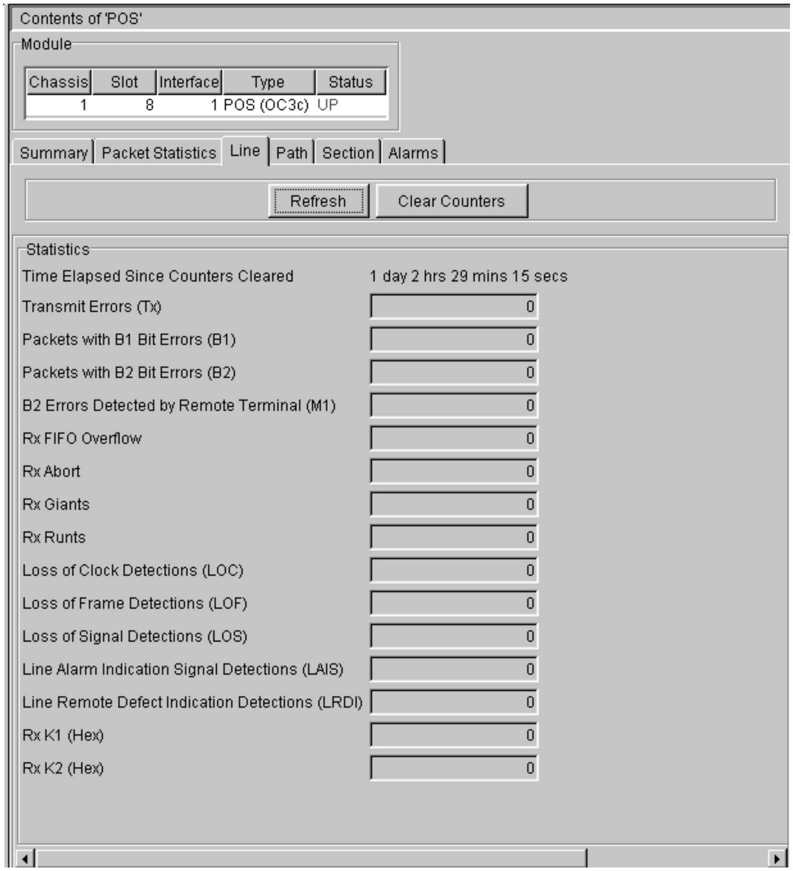
A number of performance management statistics are collected at the SONET line layer. You can view line-layer statistics for a selected POS interface by selecting the Line tab within the POS folder. The display shows counters for the basSONETLineTable as defined in the basSONET MIB.

To view Line-layer statistics for a selected POS interface, follow this procedure:

1. In the Summary window, select the interface that you want to view.
2. Select the **Line** tab.
3. Click **Refresh** to update the information.
4. Click **Clear Counters** to restart the statistics counters.

What You See

Figure 10-5 POS Line-layer Statistics Window



Contents of 'POS'

Module

Chassis	Slot	Interface	Type	Status
1	8	1	POS (OC3c)	UP

Statistics

Time Elapsed Since Counters Cleared	1 day 2 hrs 29 mins 15 secs
Transmit Errors (Tx)	0
Packets with B1 Bit Errors (B1)	0
Packets with B2 Bit Errors (B2)	0
B2 Errors Detected by Remote Terminal (M1)	0
Rx FIFO Overflow	0
Rx Abort	0
Rx Giants	0
Rx Runts	0
Loss of Clock Detections (LOC)	0
Loss of Frame Detections (LOF)	0
Loss of Signal Detections (LOS)	0
Line Alarm Indication Signal Detections (LAIS)	0
Line Remote Defect Indication Detections (LRDI)	0
Rx K1 (Hex)	0
Rx K2 (Hex)	0

Parameter Descriptions

This table provides a description of the Line window parameters.

Table 10-3 Line Window Parameters

Counter	Description
Time Elapsed Since Counters Cleared	Time *(SysUpTime)* since the counters were last cleared and reset to zero. This field shows the time in terms of `days:hours:minutes:seconds.`
Transmit Errors (Tx)	Sum of all transmit errors that caused the packet to not be transmitted. These errors consist of tx fifo error, link layer errors, minimum packet size violations, maximum packet size violations and tx parity errors.
Packets with B1 Bit Errors (B1)	Number of packets received on this link with B1 bit errors. Bit Interleaved Parity 8 is calculated over all bytes of each frame.
Packets with B2 Bit Errors (B2)	Number of packets received on this link with B2 bit errors. Bit Interleaved Parity 8 is calculated over all bytes of each frame except for the first three rows of the TOH.
B2 Errors Detected by Remote Terminal (M1)	Number of B2 errors that were detected by the remote terminal in its received signal.
Rx FIFO Overflow	Number of packets received on this link with an error detected in the receive FIFO.
Rx Abort	Number of packets received on this link in which the abort sequence is detected.
Rx Giants	Number of packets received on this link which are larger than the maximum packet size.
Rx Runts	Number of packets received on this link which are smaller than the minimum packet size.
Loss of Clock Detections (LOC)	Number of times a loss of clock has been detected. LOC occurs if no transitions are detected on the receive SONET clock for 16 periods of the transmit clock.
Loss of Frame Detections (LOF)	Number of times a loss of frame has been detected. LOF occurs if RX_OOF *(out-of-frame)* is active continuously for 24 consecutive frames (3 ms).
Loss of Signal Detections (LOS)	Number of times a loss of signal has been detected. A LOS indicates to the framer that there is no signal present from the optical receiver.

Counter	Description
Line Alarm Indication Signal Detections (LAIS)	Number of times a Line Alarm Indication Signal has been detected. A LAIS occurs if the 3 LSBs of K2 are received as '111' for 5 consecutive frames
Line Remote Defect Indication Detections (LRDI)	Number of times a Line Remote Defect Indication has been detected. A LRDI occurs if the 3 LSBs of K2 are not received as '110' for 5 consecutive frames.
Rx K1 (Hex)	K1 byte received in last packet.
Rx K2 (Hex)	K2 byte received in last packet.

Viewing SONET Path Layer Information

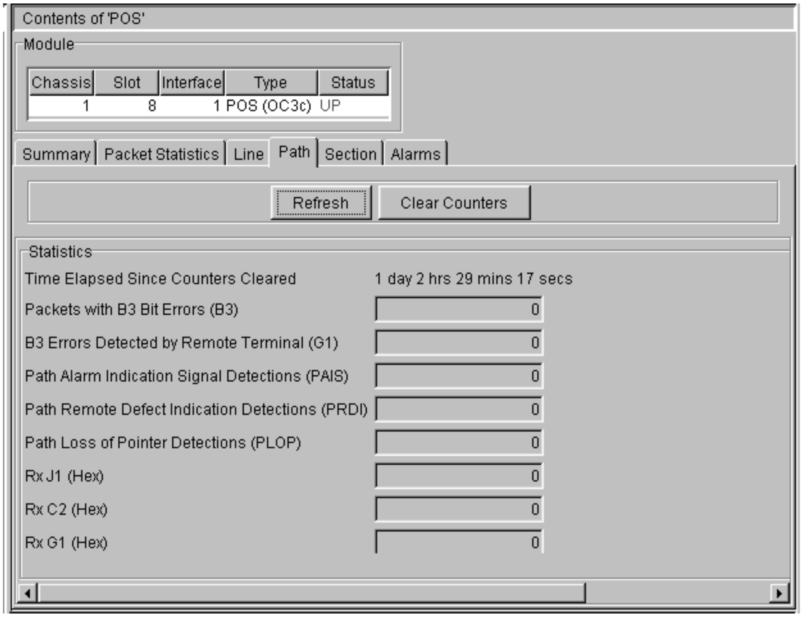
The Path layer is responsible for mapping the data to be transported into the synchronous payload envelope (SPE) of the SONET frame. It creates the STS-1 SPE and passes it to the line layer.

You can view Path-layer performance information for a selected POS interface. This information includes defects and error statistics to provide an assessment of Path layer operation. To view the Path-layer information, follow this procedure:

1. In the Summary window, select the interface that you wish to view.
2. Select the **Path** tab.
3. Click **Refresh** to update the information.
4. Click **Clear Counters** to restart the statistics counters.

What You See

Figure 10-6 Pos Path-layer Information Window



Chassis	Slot	Interface	Type	Status
1	8	1	POS (OC3c)	UP

Time Elapsed Since Counters Cleared	1 day 2 hrs 29 mins 17 secs
Packets with B3 Bit Errors (B3)	0
B3 Errors Detected by Remote Terminal (G1)	0
Path Alarm Indication Signal Detections (PAIS)	0
Path Remote Defect Indication Detections (PRDI)	0
Path Loss of Pointer Detections (PLOP)	0
Rx J1 (Hex)	0
Rx C2 (Hex)	0
Rx G1 (Hex)	0

Parameter Descriptions

This table provides a description of the POS Path-layer window statistics.

Table 10-4 POS Path-layer Window Parameters

Counter	Description
Time Elapsed Since Counters Cleared	Time *(SysUpTime)* since the counters were last cleared and reset to zero. This field shows the time in terms of `days:hours:minutes:seconds.`
Packets with B3 Bit Errors (B3)	Number of packets received on this link with B3 bit errors. Bit Interleaved Parity 8 is calculated over all bits in the SPE of each frame.
B3 Errors Detected by Remote Terminal (G1)	Number of B3 errors that were detected by the remote terminal in its received signal.

Counter	Description
Path Alarm Indication Signal Detections (PAIS)	The number of times a Path Alarm Indication Signal has been detected. A PAIS occurs if all the H1/H2 pointer bytes in the received SONET frame are 01.
Path Remote Defect Indication Detections (PRDI)	The number of times a Path Remote Defect Indication has been detected. A PRDI occurs if bits 5,6 and 7 of the G1 byte received with the same value for 5 consecutive frames.
Path Loss of Pointer Detections (PLOP)	The number of times a Path Loss of Pointer has been detected. A PLOP occurs if all the H1/H2 pointer bytes in the received SONET frame are not all 01 indicating PRDI or the first pair equals 00 and all other pairs equaling 11 indicating normal operation.
Rx J1 (Hex)	The first J1 byte received in last packet.
Rx C2 (Hex)	C2 byte received in last packet.
Rx G1 (Hex)	G1 byte received in last packet.

Section Layer Administration

The primary roles of the section layer include synchronization and timing of the SONET transmission, and passing the electrical STS frame format to the photonic layer where it is then converted to an optical signal and transported to the adjacent device.

Section layer administration involves viewing the current status of the configuration and modifying the configuration of the section layer parameters for a selected POS interface.

Before You Begin

To view the POS interface summary information, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **POS.**
2. Click the **Summary** tab.
3. Click **Refresh** to update the information.

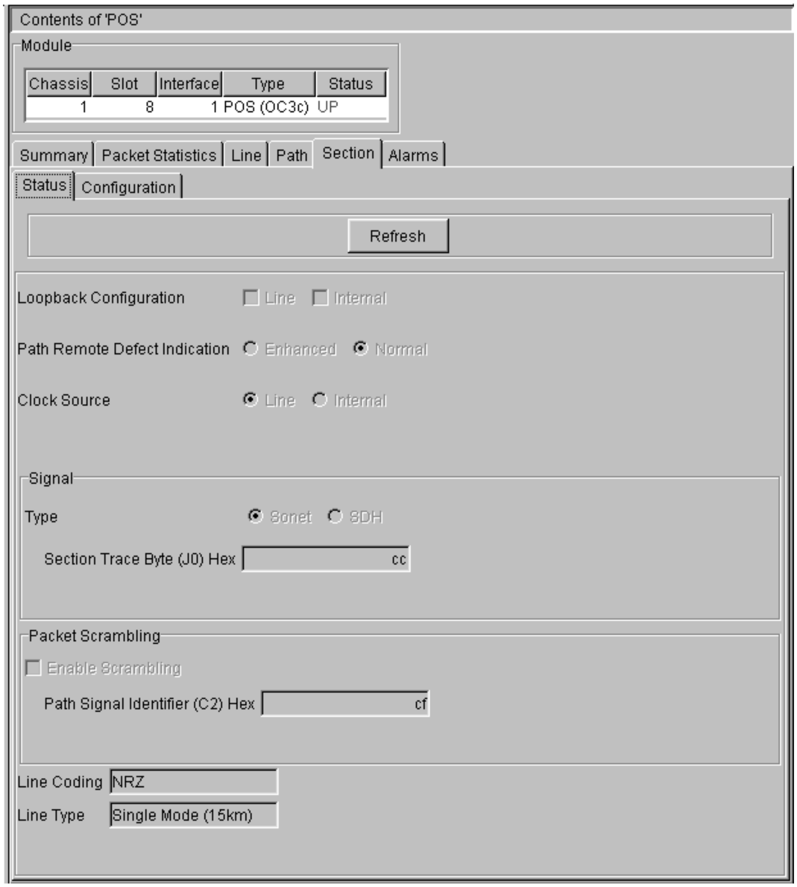
Viewing POS Section Layer Parameters

To view the POS Section Layer Parameters, follow this procedure:

1. In the Summary window, select the interface you wish to view.
2. Click the **Section** tab.
3. In the Section window, click the **Status** tab.
4. Click **Refresh** to update the information.

What You See

Figure 10-7 POS Section-layer Status Window



Contents of 'POS'

Module

Chassis	Slot	Interface	Type	Status
1	8	1	POS (OC3c)	UP

Loopback Configuration □ Line □ Internal

Path Remote Defect Indication ○ Enhanced ● Normal

Clock Source ● Line ○ Internal

Signal

Type ● Sonet ○ SDH

Section Trace Byte (J0) Hex cc

Packet Scrambling

□ Enable Scrambling

Path Signal Identifier (C2) Hex cf

Line Coding NRZ

Line Type Single Mode (15km)

Parameter Descriptions

This table provides a description of the POS Section-layer Status window

Table 10-5 POS Section-layer Status Window Parameters.

Parameter	Description
Loopback Configuration	Loopback configuration on a POS interface allows you to test interface connectivity and connection to a remote device. By default, loopback is not configured. The system supports these loopback configuration:

Parameter	Description
Line	Configures the POS interface to loop-back data to the originating device. While configured in this mode, the interface loops back and retransmits incoming data without actually receiving it.
Internal	Configures the POS interface to loop-back data to itself. While configured in this mode, the interface loops-back outgoing data to the receiver without actually transmitting it.
Path Remote Defect Indication	Configure enhanced or normal path remote defect indication on this interface *Currently not supported.*
Clock Source	SONET is a synchronous transport technology. When configuring point-to-point links, one side of the link should be configured to utilize a line clock source, the other should utilize an internal clock source. Timing for this synchronous transmission of data is derived from one of these clock sources.
Line	Also referred to as loop timing, this timing option configures the interface to use the recovered receive clock to provide transmit clocking. This is the default clock source.
Internal	Configures the interface to generate the transmit clock internally.
Signal Type	Configures the type of signal *(framing)* this POS interface transmits. Currently, the system supports only SONET STS-3c and STS-12c framing.
Packet Scrambling	Enables scrambling of SONET Synchronous Payload Envelopes (SPEs) on this interface. Note that both end-points of the transmission must use the same scrambling. Scrambling is disabled by default. Read-only.
Line Coding	This variable identifies whether a SONET or an SDH signal is used across this interface. Read-only.
Line Type	This variable describes the line coding for this interface. The B3ZS and CMI are used for electrical SONET/SDH signals (STS-1 and STS-3). The Non-Return to Zero (NRZ) and the Return to Zero are used for optical SONET/SDH signals. Read-only.

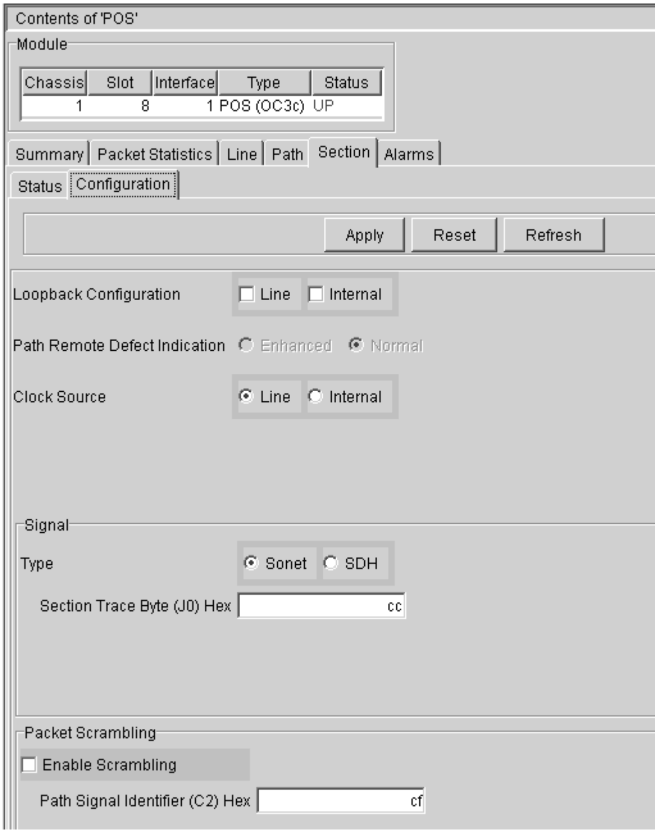
Configuring Section-Layer Parameters

To configure POS section-layer parameters, follow this procedure:

1. In the Summary window, select the interface you wish to configure.
2. Click the **Section** tab.
3. In the Section window, click the **Configuration** tab.
4. Click **Refresh** to update the information.
5. Enter values for the parameters.
6. Click **Apply** to commit the information or click **Reset** to return to the previous values.

What You See

Figure 10-8 POS Section-layer Configuration Window



Contents of 'POS'

Module

Chassis	Slot	Interface	Type	Status
1	8	1	POS (OC3c)	UP

Loopback Configuration ☐ Line ☐ Internal

Path Remote Defect Indication ○ Enhanced ● Normal

Clock Source ● Line ○ Internal

Signal

Type ● Sonet ○ SDH

Section Trace Byte (J0) Hex cc

Packet Scrambling

☐ Enable Scrambling

Path Signal Identifier (C2) Hex cf

Parameter Descriptions

This table provides a description of the POS Section-layer Configuration window parameters.

Table 10-6 POS Section-layer Configuration Window Parameters

Parameter	Description
Loopback Configuration	Loopback configuration on a POS interface allows you to test interface connectivity and connection to a remote device. By default, loopback is not configured. The system supports these loopback configuration:

Parameter	Description
Line	Configures the POS interface to loop-back data to the originating device.
Internal	Configures the POS interface to loop-back data to itself. While configured in this mode, the interface loops-back outgoing data to the receiver without actually transmitting it.
Path Remote Defect Indication	Configure path remote defect indication on this interface *At this time, only* ***Normal*** *is supported.*
Clock Source	SONET is a synchronous transport technology. When configuring point-to-point links, one side of the link should be configured to utilize a line clock source, the other should utilize an internal clock source. Timing for this synchronous transmission of data is derived from one of these clock sources.
Line	SONET timing is derived from the receiver clock.
Internal	SONET timing is derived from an internal clock source.
Signal Type	Configures the type of signal *(framing)* this POS interface transmits. Currently, the system supports only SONET STS-3c and STS-12c framing. Defaults are set to provide maximum performance. We recommend that you use the default setting.
Packet Scrambling	Enables scrambling of SONET Synchronous Payload Envelopes (SPEs) on this interface. Note that both end-points of the transmission must use the same scrambling. Scrambling is disabled by default.
Enable	Select the check box to enable packet scrambling. When enabled, the Path Signal Identifier (C2) Hex field then displays a value of *16* to indicate scrambling.
Disable	Clear the check box to disable packet scrambling. The Path Signal Identifier (C2) Hex field then displays a value of *CF* to indicate no scrambling.

Configuring and Viewing SONET Alarms

A major advantage of SONET is that it can generate alarm and error messages when problems occur, such as when a signal fails or degrades.

A receiving interface is notified of network defects in the form of Alarm Indication Signals (AIS); transmitting interfaces are notified of network defects by the return of Remote Defect Indications (RDI).

You can also access this alarm information through the Fault Management folder. For further information refer to Configuring OSPF Alarms on page 278.

Before You Begin

To view the POS interface summary information, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **POS.**
2. Click the **Summary** tab.
3. Click **Refresh** to update the information.

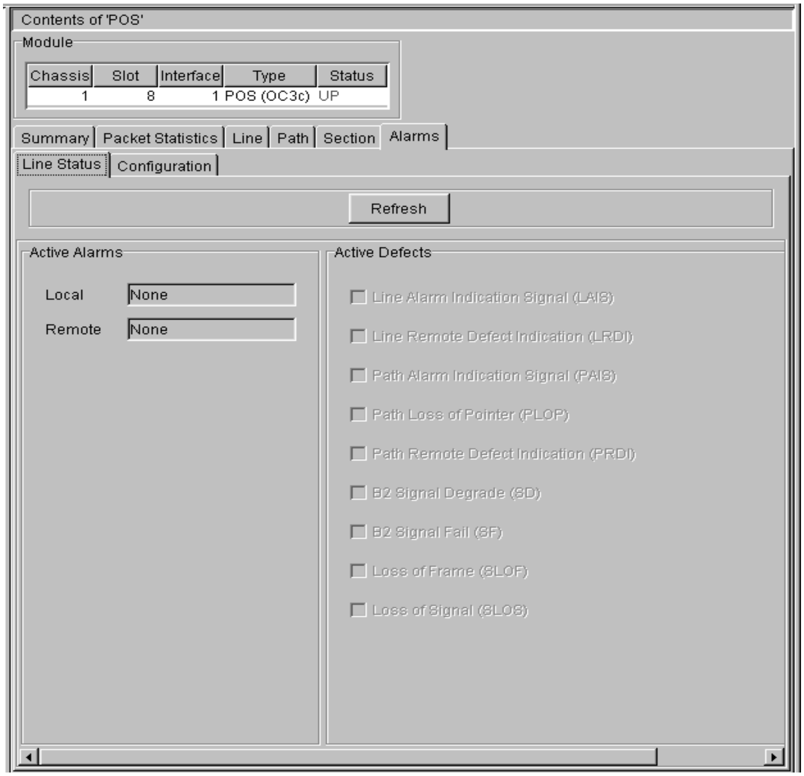
Viewing Line Status

To view the alarms and defects currently reported on a POS interface, follow this procedure:

1. In the Summary display, select the POS interface that you wish to configure.
2. Click the **Alarms** tab.
3. Click the **Line Status** tab.
4. Click **Refresh** to update the information.

What You See

Figure 10-9 POS Line Alarms Status Window



Chassis	Slot	Interface	Type	Status
1	8	1	POS (OC3c)	UP

Local: None

Remote: None

☐ Line Alarm Indication Signal (LAIS)
☐ Line Remote Defect Indication (LRDI)
☐ Path Alarm Indication Signal (PAIS)
☐ Path Loss of Pointer (PLOP)
☐ Path Remote Defect Indication (PRDI)
☐ B2 Signal Degrade (SD)
☐ B2 Signal Fail (SF)
☐ Loss of Frame (SLOF)
☐ Loss of Signal (SLOS)

Configuring SONET Alarms

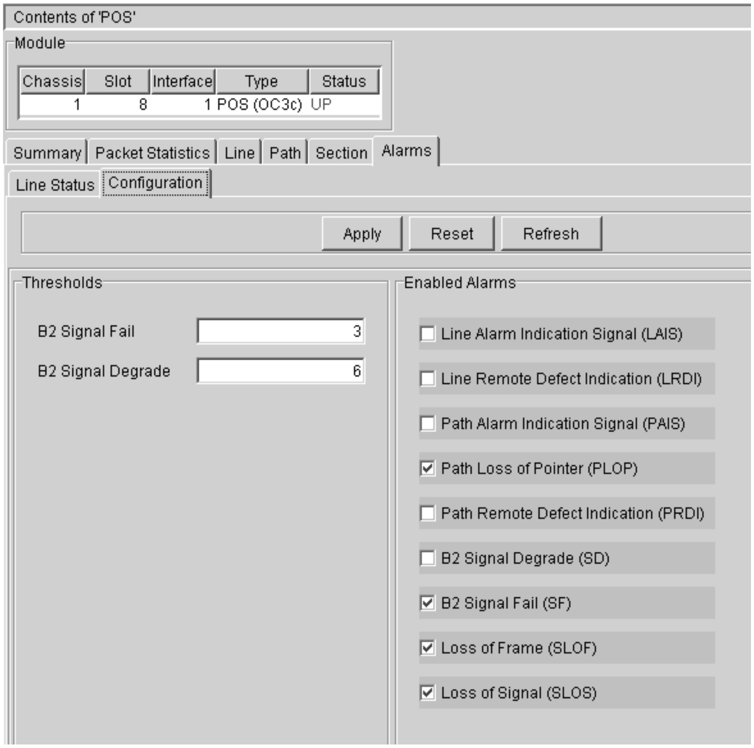
To configure the alarms and defects that you want the selected POS interface to report, follow this procedure:

1. In the Summary display, select the POS interface that you wish to configure.
2. Click the **Alarms** tab.
3. Click the **Configuration** tab.
4. Choose the alarms options that you wish the selected POS interface to report.

5. Click **Apply** to commit the information or click Reset to return to the previous values.

What You See

Figure 10-10 POS Line Alarms Configuration Window



Module

Chassis	Slot	Interface	Type	Status
1	8	1	POS (OC3c)	UP

Thresholds

B2 Signal Fail: 3

B2 Signal Degrade: 6

Enabled Alarms

- □ Line Alarm Indication Signal (LAIS)
- □ Line Remote Defect Indication (LRDI)
- □ Path Alarm Indication Signal (PAIS)
- ☑ Path Loss of Pointer (PLOP)
- □ Path Remote Defect Indication (PRDI)
- □ B2 Signal Degrade (SD)
- ☑ B2 Signal Fail (SF)
- ☑ Loss of Frame (SLOF)
- ☑ Loss of Signal (SLOS)

Parameter Descriptions

This table provides a description of the Configuration window alarms.

Table 10-7 Configuration Window Parameters

Alarm	Description
Line Alarm Indication Signal (LAIS)	Disabled by default, configures the interface to report line alarm indication signal errors.

Alarm	**Description**
Line Remote Defect Indication (LRDI)	Disabled by default, configures the interface to report line remote defect indication errors.
Path Alarm Indication Signal (PAIS)	Disabled by default, configures the system to report path alarm indication signal errors. Line terminating equipment (LTE) send packet alarm indication signals to alert downstream path terminating equipment (PTE) of defects on their incoming line signal.
Path Loss of Pointer (PLOP)	Enabled by default, configures the interface to report path loss of pointer errors. A PLOP error may result from an invalid pointer or too many new data flag enabled indications.
Path Remote Defect Indication (PRDI)	Disabled by default, configures the interface to report path remote defect indication errors.
B2 Signal Degrade (SD)	Disabled by default, configures the interface to report when the B2 signal degrades enough to meet or cross a specified Bit Error Rate (BER) threshold. Specify this threshold in the B2 Signal Degrade field on the left of the screen. The default BER threshold for B2 signal failure is 6.
B2 Signal Fail (SF)	Enabled by default, configures the interface to report a failure when the B2 signal degrades enough to meet or cross a specified Bit Error Rate (BER) threshold. Specify this threshold in the B2 Signal Fail field on the left of the screen. The default BER threshold for B2 signal failure is 3.
Loss of Frame (SLOF)	Enabled by default, configures the interface to report section loss of frame errors. The interface detects SLOF when an error on the incoming SONET signal persists for at least 3 milliseconds.
Loss of Signal (SLOS)	Enabled by default, configures the interface to report loss of signal (SLOS) errors. The POS interface reports a SLOS error under either of the following conditions: When an all-zeros pattern on the incoming SONET signal lasts at least 19(+-3) microseconds; If the signal level drops below the a specified threshold.

Configuring Point-to-Point Protocol (PPP)

PPP delivers data over SONET networks. SONET links are provisioned as point-to-point circuits. The system encapsulates IP datagrams using PPP, then places the PPP frames into the SONET payload before transmission over the SONET circuit. PPP also provides security protocols that support the authentication of peers.

PPP administration on a POS interface includes:

- Viewing PPP Summary Information — You can view a summary of all POS interfaces installed on the system and associated PPP parameters.
- Configuring PPP Security — POS interfaces support both Challenge Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP) so that only trusted devices can participate in the creation of a point-to-point circuit.
- Configuring LCP — As part of establishing the PPP connection, a POS interface uses Link Control Protocol (LCP) packets to configure and test the data link.
- Enabling NCP — A Network Control Protocol (NCP) is used to configure and enable network layer protocol communication. In this case, the network layer protocol used over the SONET circuit is IP; the NCP used to enable transmission of IP datagrams is the IP Control Protocol (IPCP).

PPP encapsulation over SONET STS-/STM-1(155 Mbps) is described in RFC 2615.

You may configure PPP and POS in either order.

Before You Begin

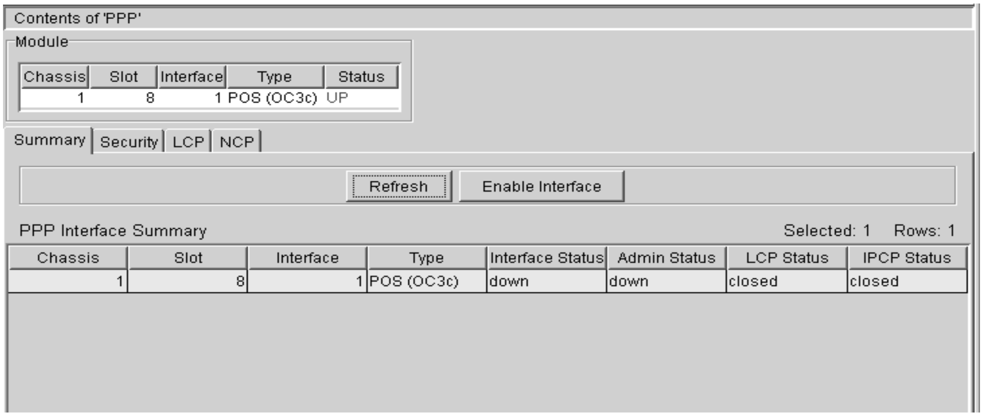
To view the PPP Administration on a POS interface summary information, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **IP** > **PPP.**
2. Click the **Summary** tab.
3. Click **Refresh** to update the information.

The Interface window provides several configuration tabs and a module information display. The module information panel, located in the top of the window, identifies the interface and the module-type currently selected.

What You See

Figure 10-11 PPP Summary window.



Contents of 'PPP'

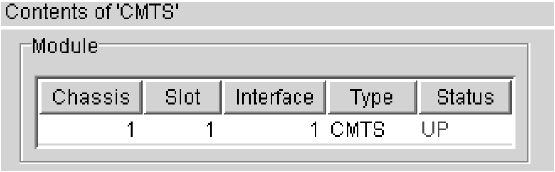
Module

Chassis	Slot	Interface	Type	Status
1	8	1	POS (OC3c)	UP

PPP Interface Summary   Selected: 1   Rows: 1

Chassis	Slot	Interface	Type	Interface Status	Admin Status	LCP Status	IPCP Status
1	8	1	POS (OC3c)	down	down	closed	closed

Figure 10-12 This figure shows an example of the Module panel.



Contents of 'CMTS'

Module

Chassis	Slot	Interface	Type	Status
1	1	1	CMTS	UP

Parameter Descriptions

This table provides a description of the PPP Summary window.

Table 10-8 PPP Summary Window Parameters

Parameter	Description
Chassis	ID of the chassis on which this interface resides.
Slot	Slot within the specified chassis on which this interface resides.
Interface	Number of this physical interface on the module *(always 1, as each POS module has a single interface)*.

Parameter	Description
Type	Type of POS interface. The system currently supports OC-3c and OC-12c interfaces.
Interface Status	Online status of this physical interface. Up indicates that the PPP connection is up; the interface can forward traffic. interface is online; down indicates that the interface is offline.
Admin Status	Administrative status of this interface. When the Administrative status is up, the interface can forward traffic. While the administrative status is down, it cannot forward traffic. To manually enable an interface, select an interface that is currently “down,” then click on the Enable Interface button at the top of the display; the interface then begins PPP negotiation. To disable an interface, select an interface that is currently “up,” then click on the Disable Interface button; the PPP connection is then brought down.
LCP Status	Link Control Status of the interface—*opened* or *closed*.
IPCP Status	IP Control Protocol (IPCP) status of this interface—*opened* or *closed*.

This table provides a description of the Module panel

Table 10-9 .Module Panel Parameters

Parameter	Description
Chassis	A unique identifying number you assigned to the chassis in the network.
Slot	Slot number in which the DOCSIS or EuroDOCSIS module is installed.
Interface	Chassis/Slot/Interface for the CMTS modules that are currently active
Type	Identifies the module as DOCSIS or EuroDOCSIS, as follows:
Euro-CMTS	Indicates a EuroDOCSIS module.
CMTS	Indicates a DOCSIS module.
Status	Indicates the operational status of the module

Configuring PPP Security

Challenge Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP) provide authentication mechanisms that serve to identify the peers that want to establish point-to-point connections. Using both CHAP and PAP, the device must provide a known *username* and *password* to the POS interface with which it wants to establish a PPP connection.

CHAP is more secure than PAP. CHAP clients respond to challenges with an encrypted version of the password; PAP sends unencrypted straight text over the network. In addition, CHAP calls for both endpoints to perform a computation to arrive at a secret string; PAP does not. You can configure the POS interface to attempt authentication using one protocol, and if refused, attempt authorization with the other.

Each CHAP and PAP must be enabled at both endpoints of a point-to-point connection and configured to operate in both client and server mode, as described in the following sections.

SONET connections are provisioned as point-to-point circuits. The connection is initiated by one peer—the caller—into an adjacent peer—the callee. The caller is referred to as the client; and the callee is referred to as the server.

Both CHAP and PAP are specified in RFC 1334.

Configuring Client-Side Security Parameters

When initiating a point-to-point connection, the POS interface acts as a client and calls into a remote end-point, which functions as a PPP server. If PAP, CHAP, or both forms of authentication are enabled and required by the server, then the same authentication protocols must be enabled on the POS interface.

The POS interface, acting as a client, must provide the remote server with the correct username and password. If the interface fails to provide the correct information, the remote device will not allow it to call in and establish a connection.

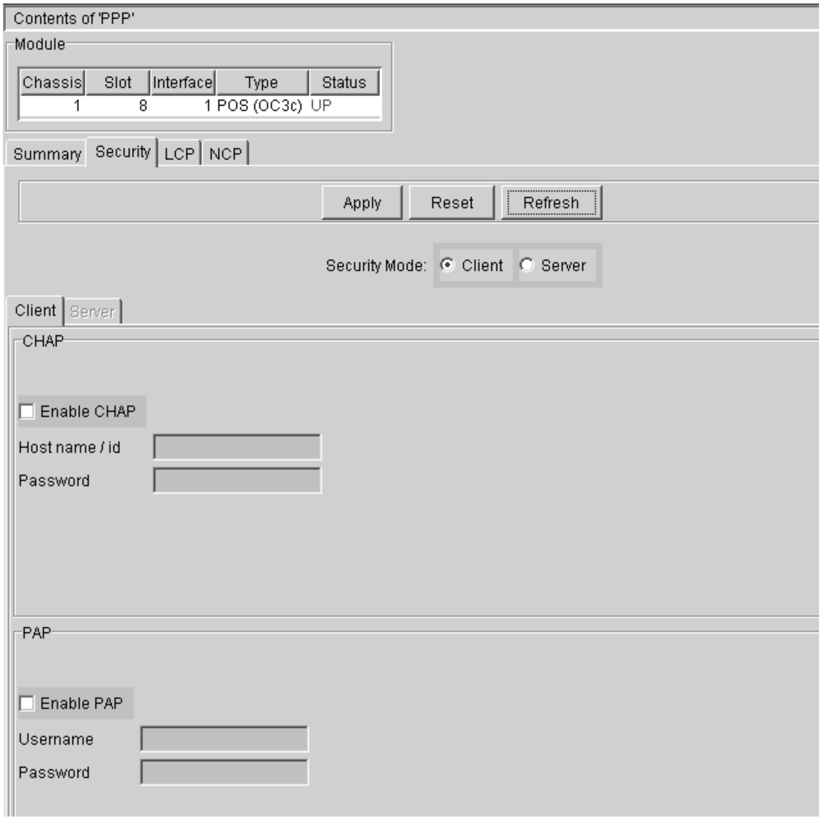
To enable client-side authentication and configure the security information—*username and password*—that the POS interface sends to a

PPP server when initiating a point-to-point connection, follow this procedure to configure a PPP client for a selected POS interface:

1. Click the **Security** tab.
2. Choose the **Security Mode: Client** option. The Client window appears.
3. Enter values for the parameters.
4. Click **Apply** to commit the information or click **Reset** to return to the previous values.
5. Click **Refresh** to update the information.

What You See

Figure 10-13 PPP Security Client Window



Contents of 'PPP'

Module

Chassis	Slot	Interface	Type	Status
1	8	1	POS (OC3c)	UP

Security Mode: ● Client ○ Server

CHAP

☐ Enable CHAP

Host name / id

Password

PAP

☐ Enable PAP

Username

Password

Parameter Descriptions

This table provides a description of the PPP Security Client window

Table 10-10 PPP Security Client Window Parameters.

Parameter	Description
Enable CHAP	Enables CHAP on the selected interface. Clear the check box to disable CHAP.
Hostname/ID	Hostname that the interface sends to a peer requiring CHAP authentication. The range is 1 to 255 alphanumeric characters.
Password	Password associated with the specified hostname.
Enable PAP	Enables PAP on the selected interface. Clear the check box to disable PAP.
Username	Username that the interface sends to remote peers requiring PAP authentication. The range is 1 to 255 alphanumeric characters.
Password	Password associated with the username to be sent to remote peers requiring PAP authentication.

Configuring Server-Side Security Parameters

When a remote peer *(client)* calls into the POS interface and attempts to establish a point-to-point connection, the interface functions as a PPP access server. Enabling server-side authentication configures the POS interface to authenticate all peers that call into it.

Configuring server-side authentication involves the following:

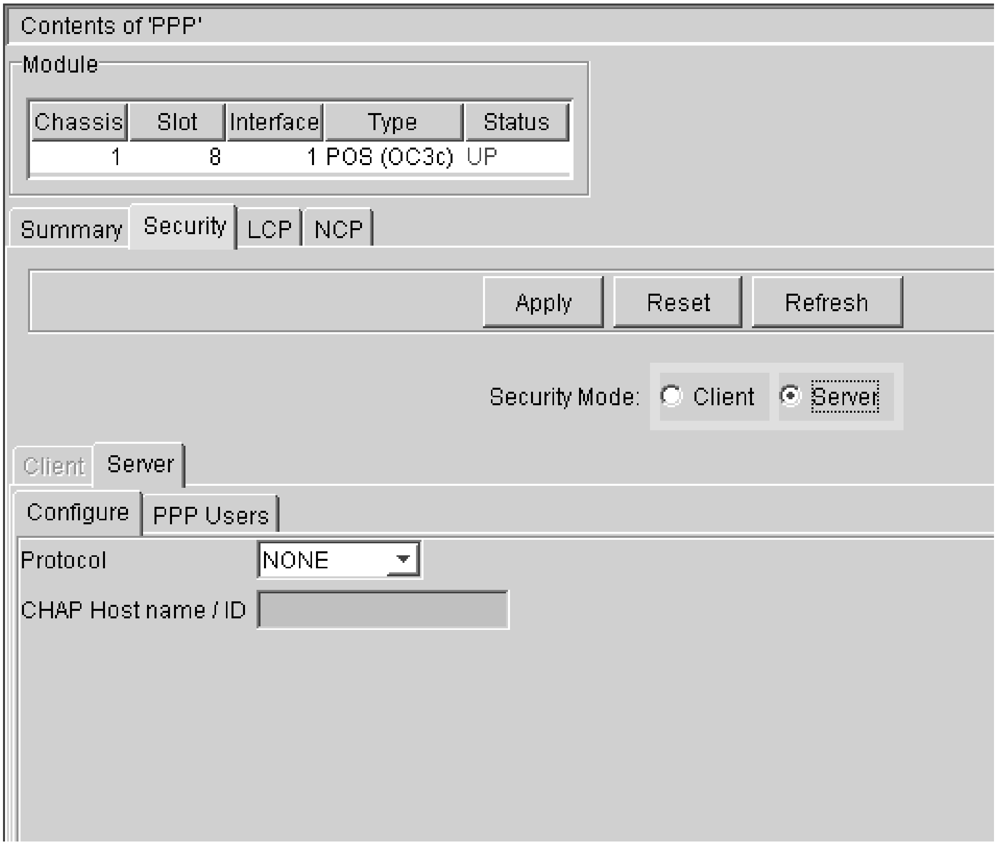
- Specifying which protocol you want the interface to use to authenticate clients. You can configure the interface to request CHAP authentication, PAP authentication, or both in a specified order.
- Specifying the hostname the POS interface sends to a client when performing CHAP authentication.
- Adding users to the *PPP LCP Server Users Table.* User account information includes a username and password. When a remote client responds to a PAP challenge with a username and password, the system examines this table to verify that the client has responded with the correct information. If so, the connection is allowed; otherwise, the connection is closed.

Follow this procedure to configure PPP server-side security parameters for a selected POS interface:

1. Click the **Security** tab.
2. Choose the **Security Mode: Server** option. The Server window appears.
3. Click **Configure**
4. Enter values for the parameters.
5. Click **Apply** to commit the information or click **Reset** to return to the previous values.
6. Click **Refresh** to update the information.
7. If you have selected PAP or CHAP *(or an option containing PAP)* as the authentication protocol, you must configure user accounts as described in the next section, *"Configuring PPP Users."*

What You See

Figure 10-14 PPP Security Server Configure Window



Contents of 'PPP'

Module

Chassis	Slot	Interface	Type	Status
1	8	1	POS (OC3c)	UP

Security Mode: ○ Client ● Server

Protocol: NONE

CHAP Host name / ID:

Parameter Descriptions

This table provides a description of the PPP Security Server Configure window.

Table 10-11 PPP Security Server Configure Window Parameters

Parameter	Description
Protocol	
None	Server side authentication is disabled. This means that the interface does not authenticate peers that call into it.

Parameter	Description
PAP	Enables PAP on the current POS interface.
PAP-CHAP	Enables both PAP and CHAP. Enabling both authentication protocols allows for the interface to negotiate which one it uses to identify a remote entity. The interface requests PAP authentication first. If the remote entity is not configured or refuses PAP authentication, the interface then requests CHAP authentication. If CHAP authentication is rejected as well, the interface cannot authenticate the host and therefore does not allow the connection.
CHAP	Enables CHAP on the current POS interface.
CHAP-PAP	Enables both CHAP and PAP. Enabling both authentication protocols allows for the interface to negotiate which one it uses to identify a remote entity. The interface requests CHAP authentication first. If the remote entity is not configured or refuses CHAP authentication, the interface then requests PAP authentication. If PAP authentication is rejected as well, the interface cannot authenticate the host and therefore does not allow the connection.
CHAP Host Name / ID	If you have selected CHAP *(or an option containing CHAP)* as the authentication protocol, you must enter the hostname the server will use in the field.

Configuring PPP Users

If you configured the interface to authenticate peers using CHAP or PAP, then you must add user account information for all peers that the interface may authenticate.

When CHAP or PAP is enabled for server mode, the interface requests a username and password from the remote peer. When the peer responds with a username/password combination, the POS interface examines its *PPP LCP Server Users Table* to verify the information is correct. If the account information is verified correct, the connection is allowed; otherwise it’s closed.

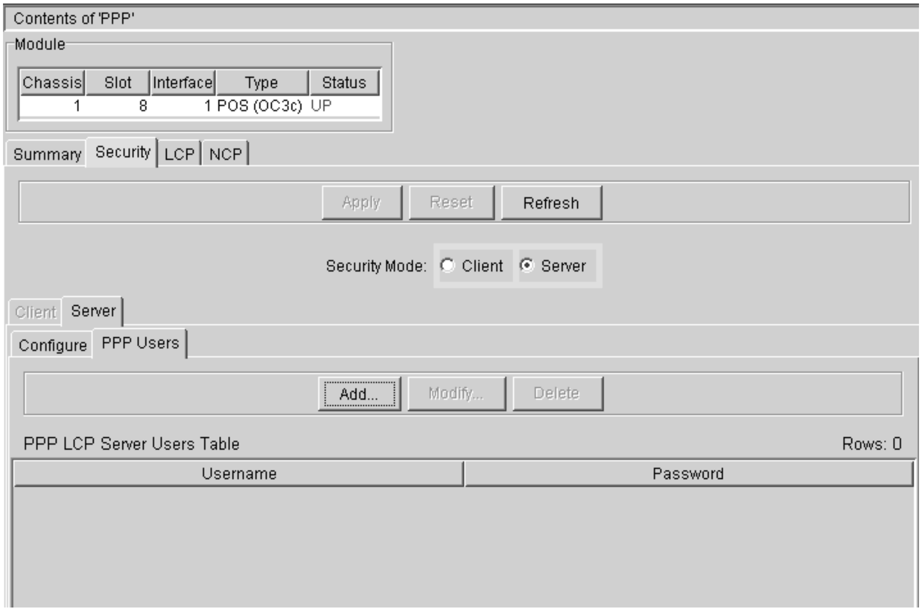
Adding a PPP User Account

To add a user to the PPP LCP Server Users Table of a selected interface, follow this procedure:

1. Click the **Security** tab.
2. Choose the **Security Mode: Server** option. The Server window appears.
3. Click the **PPP Users** tab.
4. Click the **Add** button. The Add User window appears.
5. Enter the Username and Password for the user account.
6. Click **Ok** to commit the information or click **Cancel** to exit without saving.

What You See

Figure 10-15 PPP Users Window



Contents of 'PPP'

Module

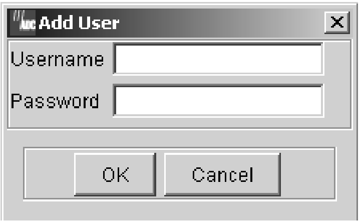
Chassis	Slot	Interface	Type	Status
1	8	1	POS (OC3c)	UP

Security Mode: ○ Client ● Server

PPP LCP Server Users Table Rows: 0

Username	Password

Figure 10-16 PPP: Add User window.



Modifying a PPP User Account

To modify a PPP user account, follow this procedure:

1. In the Summary window, select the interface that you wish to configure.
2. Click the **Security** tab.
3. Choose the **Security Mode: Server** option. The Server window appears.
4. Click the **PPP Users** tab.
5. Click the **Modify** button. The Add User window appears.
6. Update the Username and Password for the user account.
7. Click **Ok** to commit the information or click **Cancel** to exit without saving.

Deleting a PPP User Account

When you no longer need an account, or want to ensure that a peer does not connect to the interface when PPP authentication is enabled, you can delete the user account. To delete a PPP user account, follow this procedure:

1. In the Summary window, select the interface that you wish to configure.
2. Click the **Security** tab.
3. Choose the **Security Mode: Server** option. The Server window appears.
4. Click the **PPP Users** tab.
5. Click the **Delete** button. A confirmation window appears.
6. Click **Yes** to delete the user account or click **No** to cancel the deletion.

Configuring LCP

The PPP protocol suite includes a Link Control Protocol (LCP) for establishing, configuring and verifying point-to-point connections. PPP uses LCP to determine encapsulation options, set limits in transmit and receive packet size, detect link configuration errors, and terminate links.

LCP is defined in RFCs 1570 and 1661.

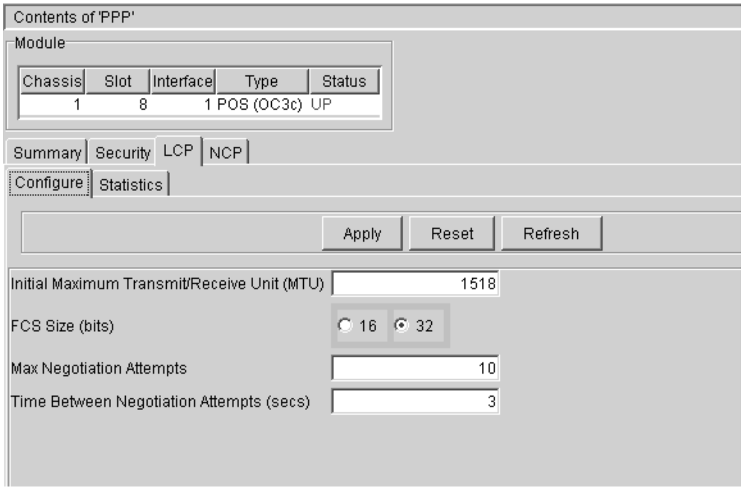
Configuring LCP Parameters

To configure LCP parameters for a selected PPP interface, follow this procedure:

1. Click the **LCP** tab.
2. Click the **Configure** tab. The Configure window appears.
3. Click **Apply** to commit the information or click **Reset** to return to the previous values.

What You See

Figure 10-17 LCP Configure Window



Contents of 'PPP'

Module

Chassis	Slot	Interface	Type	Status
1	8	1	POS (OC3c)	UP

Initial Maximum Transmit/Receive Unit (MTU) 1518

FCS Size (bits) ○ 16 ● 32

Max Negotiation Attempts 10

Time Between Negotiation Attempts (secs) 3

Parameter Descriptions

This table provides a description of the Configure window parameters

Table 10-12 Configure Window Parameters.

Parameter	Description
Initial Maximum Transmit / Receive Unit (MTU)	maximum transmit and receive packet size allowed on this interface. This release supports a MTU size of 1500 only. Note that IP packets are encapsulated in PPP. This means the maximum length of an IP packet that can be transmitted over the PPP link is the same length as the PPP information field. If a packet is larger than the PPP information field, it must be fragmented and placed in multiple PPP packets.
FCS Size (bits)	Sets the Frame Check Sequence (FCS) size. The options are: 16 or 32
Max Negotiation Attempts	Maximum number of link negotiation attempts allowed by this interface.
Time Between Negotiation Attempts (secs)	Time, in seconds, that the interface waits between LCP negotiations.

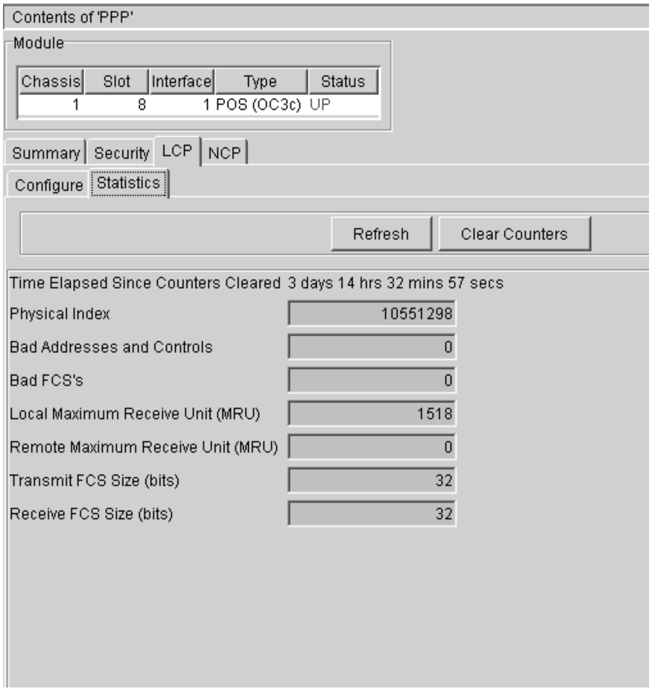
Viewing LCP Statistics

You can view LCP counters for a selected POS interface. The display shows LCP statistics as defined in RFC 1471. To view LCP statistics for a selected POS interface, follow this following procedure.

1. Click the **LCP** tab.
2. Click the **Statistics** tab. The Statistics window appears.
3. Click **Refresh** to update the information.
4. Click **Clear Counters** to restart all counters.

What You See

Figure 10-18 LCP Statistics Window



Contents of 'PPP'

Module

Chassis	Slot	Interface	Type	Status
1	8	1	POS (OC3c)	UP

Time Elapsed Since Counters Cleared	3 days 14 hrs 32 mins 57 secs
Physical Index	10551298
Bad Addresses and Controls	0
Bad FCS's	0
Local Maximum Receive Unit (MRU)	1518
Remote Maximum Receive Unit (MRU)	0
Transmit FCS Size (bits)	32
Receive FCS Size (bits)	32

Parameter Descriptions

This table provides a description of the Statistics window parameters.

Table 10-13 Statistics Window Parameters

Parameter	Description
Time Elapsed Since Counters Cleared	Time (SysUpTime) since the counters were last cleared and reset to zero. The Clear Counters button clears all SONET/SDH counters for the selected POS interface.
Physical Index	Index number that identifies the lower-level interface over which this PPP Link is operating.
Bad Addresses and Controls	Number of packets discarded because they were received with incorrect address or control fields. Address field was not 0xFF or control field was not 0x03.

Parameter	Description
Bad FCS's	Number of received packets that have been discarded due to having an incorrect FCS.
Local Maximum Receive Unit (MRU)	Current value of the MRU for the local PPP Entity. The remote entity uses this MRU when sending packets to the local PPP entity. Value is meaningful only when the link has reached the *open* state
Remote Maximum Receive Unit (MRU)	Current value of the MRU for the remote PPP Entity. The interface uses this MRU when sending packets to the remote PPP entity. Value is only meaningful when the link has reached the *open* state.
Transmit FCS Size (bits)	Frame Check Sequence (FCS) in bits that the local entity generates when sending packets to the remote entity. Value is only meaningful when the link has reached the open state.
Receive FCS Size (bits)	Size of the Frame Check Sequence (FCS) in bits that the remote entity generates when sending packets to the local entity. Value is only meaningful when the link has reached the open state.

Enabling NCP

IP Control Protocol (IPCP) is the Network Control Protocol (NCP) used to configure, enable, and disable IP protocol access on both ends of a SONET point-to-point circuit. In order for IP packets to be transmitted over the point-to-point link, IPCP must reach the open state. This enables IP communication between the two circuit endpoints.

By default, the Cuda 12000 is configured to provide its IP address during IPCP negotiations. But when negotiating with a Juniper Networks system, providing the IP address during IPCP negotiation prevents a successful connection.

When the interface must connect with a Juniper Networks system, you can disable reporting of an IP address during IPCP negotiation. To *enable* or *disable* reporting of the IP address during negotiation, follow this procedure:

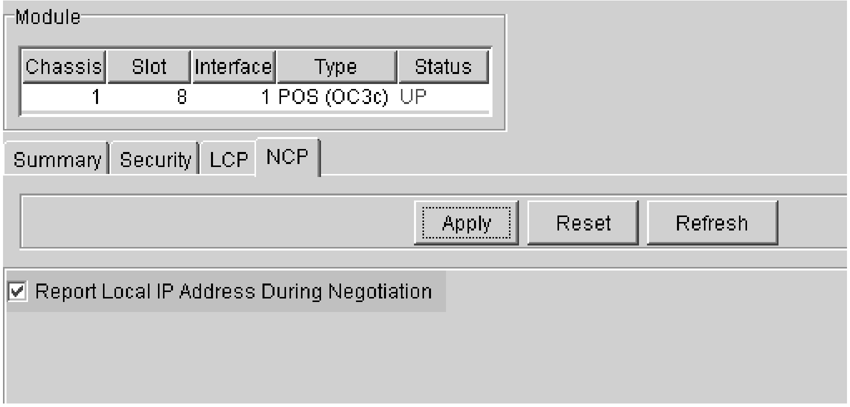
1. In the Summary window, select the interface that you wish to configure.
2. Click the **NCP** tab.
3. Enable or disable reporting of the IP address during IPCP negotiation by selecting the Report Local IP Address During Negotiation option. When

selected, IP address reporting is enabled. When the check box is clear, reporting is disabled.

4. Click **Apply** to commit the information or click **Reset** to return to the previous values.
5. Click **Refresh** to update the information.

What You See

Figure 10-19 NCP Window



Module

Chassis	Slot	Interface	Type	Status
1	8	1	POS (OC3c)	UP

☑ Report Local IP Address During Negotiation

11 FAULT MANAGEMENT

This chapter explains fault management and backplane clock sources on the Cuda 12000, and includes the following sections:

- About Fault Management
- Alarm Tables
- Alarm Management
- Configuring Hardware Alarms
- Configuring Fault Reporting
- Configuring for Backplane Clock Sources

About Fault Management

The Cuda 12000 supports fault management, a function that uses the management module to allow you to discover and manage cable modem, module, and link fault events.

Fault Management allows you to:

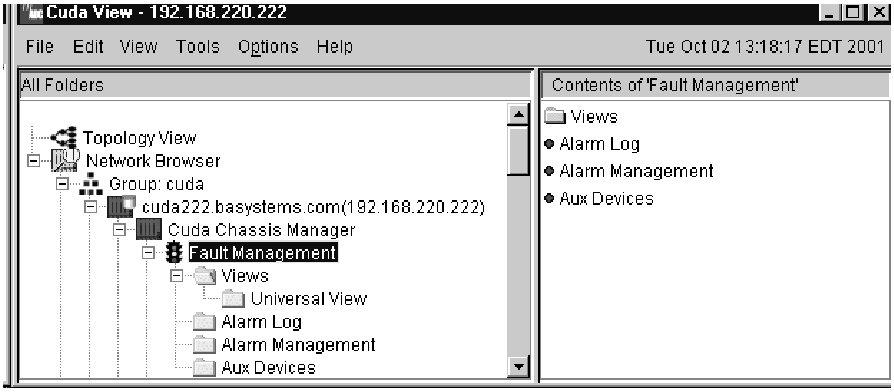
- View the Cuda 12000 chassis
- Use Alarms to discover fault events
- Manage fault events with the Alarm Log

Before You Begin

Before you begin, navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Fault Management.**

What You See

Figure 11-1 Fault Management Folder Window



Universal View

The purpose of the Universal View is to display a minimized view of the front of the Cuda 12000 chassis, and to notify you of the alarms. Double-click on the Universal View folder to display a minimized view of the chassis.

To access the chassis view, follow this procedure:

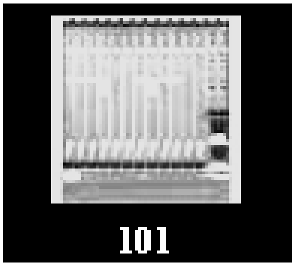
1. In the Fault Management menu item, select the Universal View item. A minimized view of the Cuda 12000 chassis appears.
2. To view the maximized chassis view, double-click on the picture. The maximized view allows you to identify the chassis and displays each module. A module that sends an alarm has been colored according to its fault event. The view also shows the identifying chassis numbers, which are located at the top left corner of the chassis: The examples includes:

- 101 — A number assigned dynamically to the cluster.
- 1/ — User-defined unique id number assigned to the chassis within the network.
- 13/ — Slot number that contains the management module.
- 0/ —Internal management interface number.
- 1 — Type of logical port on this interface. "1" indicates a main processor. "2" indicates a daughter module processor.

What You See

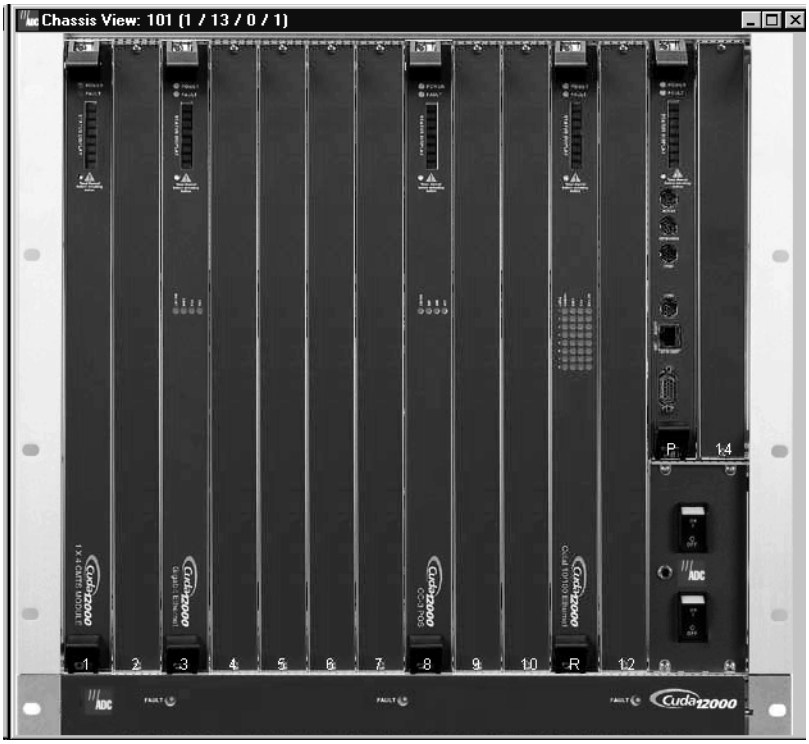
This figure is a minimized view of the front of the Cuda 12000 chassis.

Figure 11-2 Universal View - Minimized



To see the maximized chassis view, double-click on the picture. The maximized view allows you to identify the chassis.

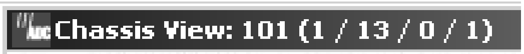
This figure is a maximized view.



Chassis View: 101 (1 / 13 / 0 / 1)

This figure shows the identifying numbers in the front of the Cuda 12000 chassis.

Figure 11-3 Chassis ID Numbers



Chassis View: 101 (1 / 13 / 0 / 1)

Alarms

Fault Management works by sending out Alarms to represent a fault event. Application modules generate the alarms to the management module, and notify you that a module is experiencing a fault event. The Alarms use a color-coded scheme to identify the severity of the fault, which is:

- Red — Indicates a Critical event — for example, a link is down
- Orange — Indicates a Major event — for example, a module is down
- Yellow — Indicates a Minor event — for example, a modem is down

- White — Indicates a Normal event, and includes various issues.

It is easier to display the alarm colors in the maximized chassis view. In minimized view, the entire chassis is the color of the most severe fault event *(critical being most severe to minor being least severe)*. There may also be other less severe faults occurring at the same time, which you cannot see in minimized view.

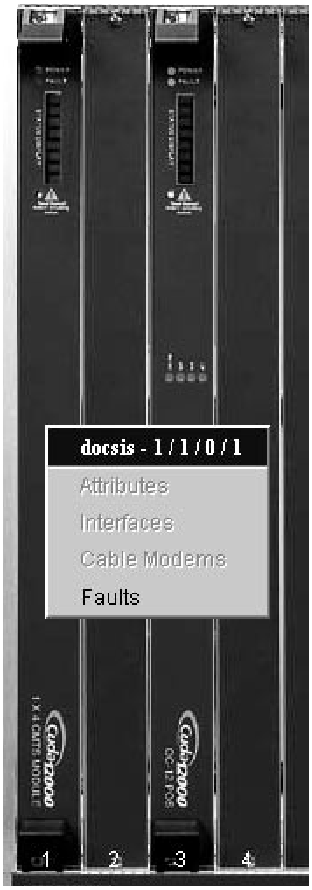
Displaying Alarm Severity and Fault Events

To display the fault event on a module, follow this procedure:

1. In the Universal View window, double click on the chassis. The maximized view appears.
2. Right click on the particular module. A dialogue box appears to identify the module and lists a Faults command.
3. Click **Faults** or double-click on the module. The Alarm table appears. The Alarm Table identifies the severity of the alarm and provides the description of the fault event that is occurring on that module.

What You See

This figure is an example of a command menu with the Faults command. The contents of the menu depends upon the particular module thus selected.



Alarm Tables

The Alarm Table allows you to view all the alarm notifications *(sent in the form of SNMP Traps and syslog messages)* that the management module receives. It also allows you to update the status of Traps as you address them, and purge (delete) traps when you no longer need them. There are three Alarm Table views, as follows:

- Chassis View — Display the Alarm Table for the entire chassis. You can only display the chassis view from the Views folder.
- Card View — Display the Alarm Table for only a module. You can only display the chassis view from the Views folder.
- Alarm Log View — Displays the Alarm log for all modules and software. You can only display the chassis view from the Alarm Log folder.

Alarms are displayed only during client runtime. There is no alarm history.

Before You Begin

Before you begin to view the alarm tables, navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Fault Management.**

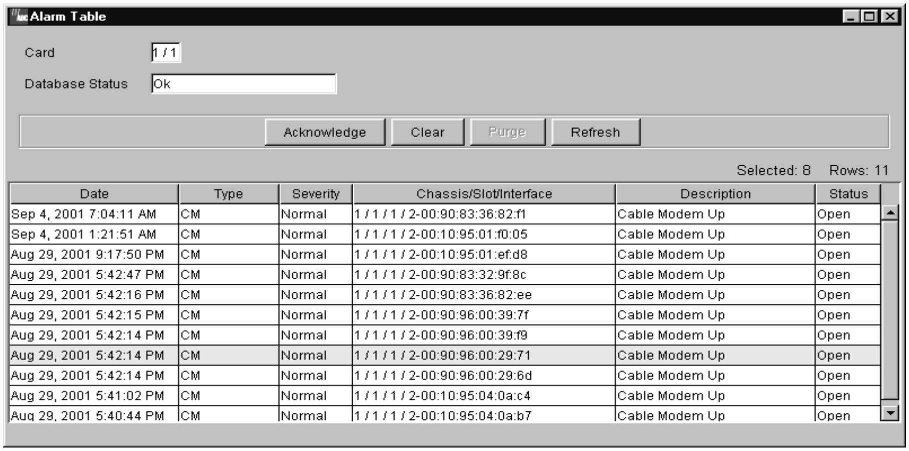
Viewing Module and Chassis Faults

To view the Card and Chassis Alarm Tables use these procedures:

1. From the Fault Management folder, navigate to **Views** > **Universal View.**
2. Open the Universal View folder, and double-click on the graphic of the chassis to display the maximized chassis view.
3. To display the Alarm Table for a selected module, double-click on the desired module to display an Alarm Table. The alarm table for the selected module appears (Figure 11-4.)
4. To display the Alarm Table by Chassis View, double-click on the left or right view of the mounting bracket of the chassis. The alarm table for the chassis appears (Figure 11-5).

What You See

Figure 11-4 Card View Alarm Table



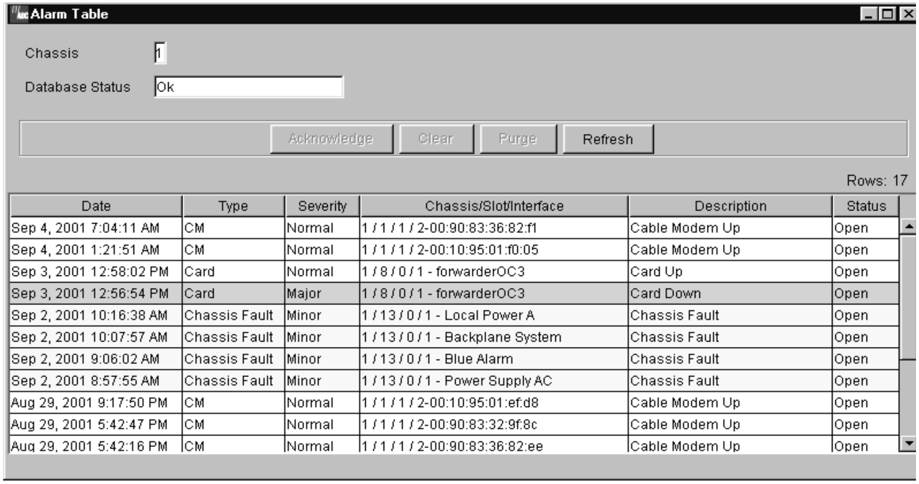
Card 1 / 1

Database Status Ok

Selected: 8 Rows: 11

Date	Type	Severity	Chassis/Slot/Interface	Description	Status
Sep 4, 2001 7:04:11 AM	CM	Normal	1 / 1 / 1 / 2-00:90:83:36:82:f1	Cable Modem Up	Open
Sep 4, 2001 1:21:51 AM	CM	Normal	1 / 1 / 1 / 2-00:10:95:01:f0:05	Cable Modem Up	Open
Aug 29, 2001 9:17:50 PM	CM	Normal	1 / 1 / 1 / 2-00:10:95:01:ef:d8	Cable Modem Up	Open
Aug 29, 2001 5:42:47 PM	CM	Normal	1 / 1 / 1 / 2-00:90:83:32:9f:8c	Cable Modem Up	Open
Aug 29, 2001 5:42:16 PM	CM	Normal	1 / 1 / 1 / 2-00:90:83:36:82:ee	Cable Modem Up	Open
Aug 29, 2001 5:42:15 PM	CM	Normal	1 / 1 / 1 / 2-00:90:96:00:39:7f	Cable Modem Up	Open
Aug 29, 2001 5:42:14 PM	CM	Normal	1 / 1 / 1 / 2-00:90:96:00:39:f9	Cable Modem Up	Open
Aug 29, 2001 5:42:14 PM	CM	Normal	1 / 1 / 1 / 2-00:90:96:00:29:71	Cable Modem Up	Open
Aug 29, 2001 5:42:14 PM	CM	Normal	1 / 1 / 1 / 2-00:90:96:00:29:6d	Cable Modem Up	Open
Aug 29, 2001 5:41:02 PM	CM	Normal	1 / 1 / 1 / 2-00:10:95:04:0a:c4	Cable Modem Up	Open
Aug 29, 2001 5:40:44 PM	CM	Normal	1 / 1 / 1 / 2-00:10:95:04:0a:b7	Cable Modem Up	Open

Figure 11-5 Chassis View Alarm Table



Chassis 1

Database Status Ok

Rows: 17

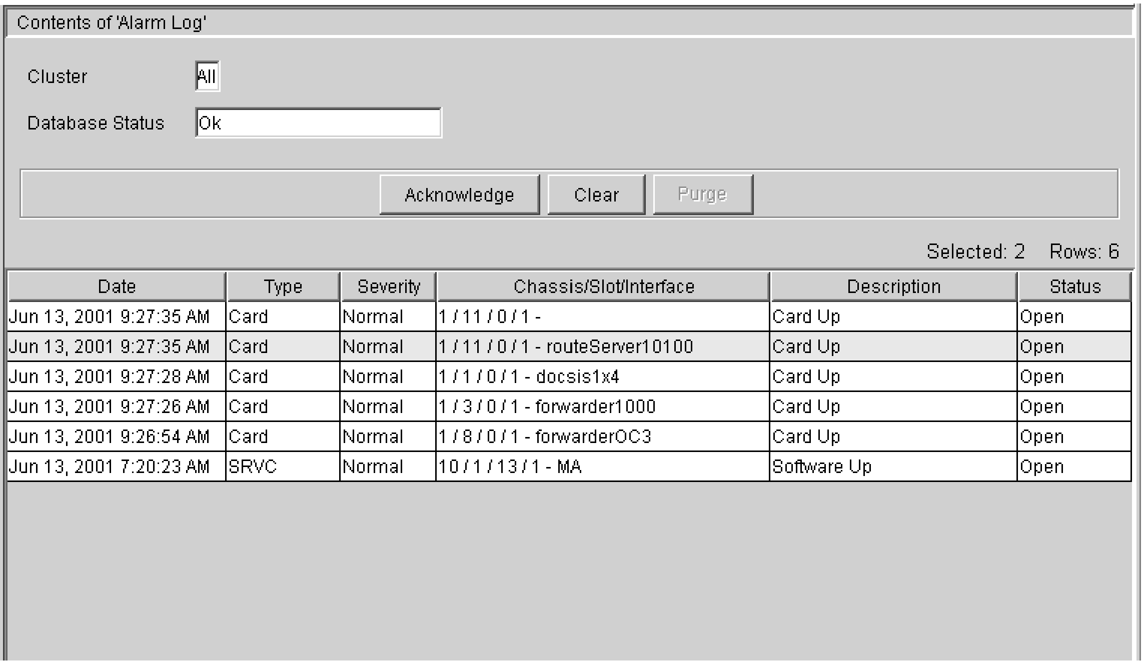
Date	Type	Severity	Chassis/Slot/Interface	Description	Status
Sep 4, 2001 7:04:11 AM	CM	Normal	1 / 1 / 1 / 2-00:90:83:36:82:f1	Cable Modem Up	Open
Sep 4, 2001 1:21:51 AM	CM	Normal	1 / 1 / 1 / 2-00:10:95:01:f0:05	Cable Modem Up	Open
Sep 3, 2001 12:58:02 PM	Card	Normal	1 / 8 / 0 / 1 - forwarderOC3	Card Up	Open
Sep 3, 2001 12:56:54 PM	Card	Major	1 / 8 / 0 / 1 - forwarderOC3	Card Down	Open
Sep 2, 2001 10:16:38 AM	Chassis Fault	Minor	1 / 13 / 0 / 1 - Local Power A	Chassis Fault	Open
Sep 2, 2001 10:07:57 AM	Chassis Fault	Minor	1 / 13 / 0 / 1 - Backplane System	Chassis Fault	Open
Sep 2, 2001 9:06:02 AM	Chassis Fault	Minor	1 / 13 / 0 / 1 - Blue Alarm	Chassis Fault	Open
Sep 2, 2001 8:57:55 AM	Chassis Fault	Minor	1 / 13 / 0 / 1 - Power Supply AC	Chassis Fault	Open
Aug 29, 2001 9:17:50 PM	CM	Normal	1 / 1 / 1 / 2-00:10:95:01:ef:d8	Cable Modem Up	Open
Aug 29, 2001 5:42:47 PM	CM	Normal	1 / 1 / 1 / 2-00:90:83:32:9f:8c	Cable Modem Up	Open
Aug 29, 2001 5:42:16 PM	CM	Normal	1 / 1 / 1 / 2-00:90:83:36:82:ee	Cable Modem Up	Open

Viewing the Alarm Log

To view the Alarm Log for the modules and software, navigate to the Alarm Log folder in the Fault Management folder. The Alarm Log for cluster appears.

What You See

Figure 11-6 Alarm Log window.



Contents of 'Alarm Log'

Cluster: All

Database Status: Ok

Selected: 2 Rows: 6

Date	Type	Severity	Chassis/Slot/Interface	Description	Status
Jun 13, 2001 9:27:35 AM	Card	Normal	1 / 11 / 0 / 1 -	Card Up	Open
Jun 13, 2001 9:27:35 AM	Card	Normal	1 / 11 / 0 / 1 - routeServer10100	Card Up	Open
Jun 13, 2001 9:27:28 AM	Card	Normal	1 / 1 / 0 / 1 - docsis1x4	Card Up	Open
Jun 13, 2001 9:27:26 AM	Card	Normal	1 / 3 / 0 / 1 - forwarder1000	Card Up	Open
Jun 13, 2001 9:26:54 AM	Card	Normal	1 / 8 / 0 / 1 - forwarderOC3	Card Up	Open
Jun 13, 2001 7:20:23 AM	SRVC	Normal	10 / 1 / 13 / 1 - MA	Software Up	Open

Parameter Descriptions

This table provides a description of the Alarm Log window

Table 11-1 . Alarm Log Window Parameters

Parameter	Description
Cluster	Identifies what view you choose. The options are: Module, Chassis, Cluster, or All.
Database Status	Indicates whether the size of the Alarm Log database has exceeded acceptable limits. If within acceptable limits, the status is displayed as Ok. If the Alarm Table database exceeds acceptable limits, the percentage of the database that is utilized is shown in this field.
Date	Date and time that the event occurs and the Trap is generated.
Type	Type of event.

Parameter	Description
Severity	Severity level of the event. The options are: Critical, Major, Minor, or Normal.
Chassis/Slot/Interface	The interface on which the event occurred.
Description	Description of the event.
Status	Administrative status of the event. The administrative status allows you to communicate with other administrators and keep track of the events as you address them. The three stages of administrative status include: Open — Dynamically set by the system when the event occurs. It indicates that the event has not received administrative attention, or at least has not been officially labelled as receiving attention. Acked — Provides a mechanism for the administrator to indicate that the Alarm event has been acknowledged and is being addressed. To mark alarm events as acknowledged (Acked), select the row/s that include the alarm events that you want to acknowledge and click Acknowledge. Clear — Provides a mechanism for the administrator to indicate that the Alarm event is resolved. To mark alarm events as cleared, select the row or rows that include the alarm events that you want clear and click Clear.

Purging Events from the Alarm Log

You can purge (delete) entries that have an administrative status of clear. To purge one or more events, follow this procedure:

1. In the Alarm Log window, make sure that the events you wish to purge are marked as clear.
2. Click **Purge**. The system deletes all cleared events from the Alarm database.

Alarm Management

The Cuda 12000 allows you to configure alarms to identify fault events. These alarms can notify you of potential fault conditions or configuration errors that may impact system performance and network health.

Before You Begin

Before you begin navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Fault Management** > **Alarm Management.**

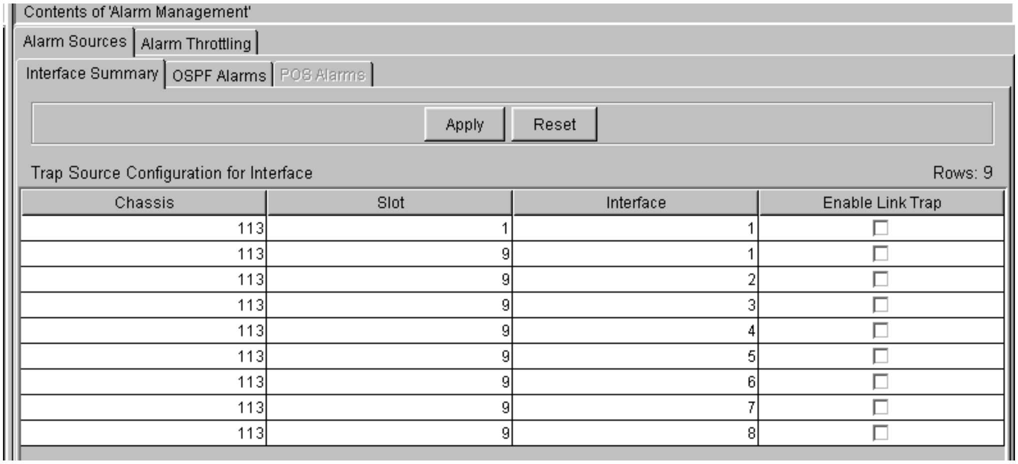
Configuring Trap Sources

To configure trap sources for an interface, follow this procedure:

1. In the Alarm Management window, click the **Alarm Sources** tab.The **Interface Summary** window appears.
2. In the Enable Link Trap column, select the interface that you wish to enable as the link trap. By selecting the check box, the link trap is enabled. By clearing the check box, the link trap is disabled.
3. Click **Apply** to commit the information or click **Reset** to return to the previous values.

What You See

Figure 11-7 Alarm Sources Interface Summary window.



Contents of 'Alarm Management'

Trap Source Configuration for Interface

Rows: 9

Chassis	Slot	Interface	Enable Link Trap
113	1	1	□
113	9	1	□
113	9	2	□
113	9	3	□
113	9	4	□
113	9	5	□
113	9	6	□
113	9	7	□
113	9	8	□

Configuring OSPF Alarms

OSPF alarms refer to events that indicate a change in the state of OSPF neighbors and OSPF virtual neighbors.

Parameter Descriptions

The following table describes the OSPF alarms:

Table 11-2 OSPF Alarms

Parameter	Description
OSPF Neighbor State Change	Indicates a change in the state of an OSPF neighbor on a physical interface.
OSPF Virtual Neighbor State Change	Indicates a change in the state of an OSPF neighbor on a virtual interface.

To configure the OSPF alarms that you want the selected interface to report, follow this procedure:

1. In the Interface Summary window, select the interface that you wish to configure.
2. Click the **OSPF Alarms** tab.
3. Select OSPF Neighbor State Change if you want the selected interface to report the change in state of an OSPF neighbor on a physical interface. Deselect this option if you do not want to receive a report.
4. Select OSPF Virtual Neighbor State Change if you want the selected interface to report the change in state of an OSPF neighbor on a virtual interface. Deselect this option if you do not want to receive a report.
5. Click **Apply** to commit the information or click **Reset** to return to the previous values.

Configuring and Viewing SONET Alarms

A major advantage of SONET is that it can generate alarm and error messages when problems occur, such as when a signal fails or degrades.

A receiving interface is notified of network defects in the form of Alarm Indication Signals (AIS); transmitting interfaces are notified of network defects by the return of Remote Defect Indications (RDI).

You can also access this alarm information through the POS folder. For further information refer to Chapter 10, “Packet Over SONET Administration” on page 278.

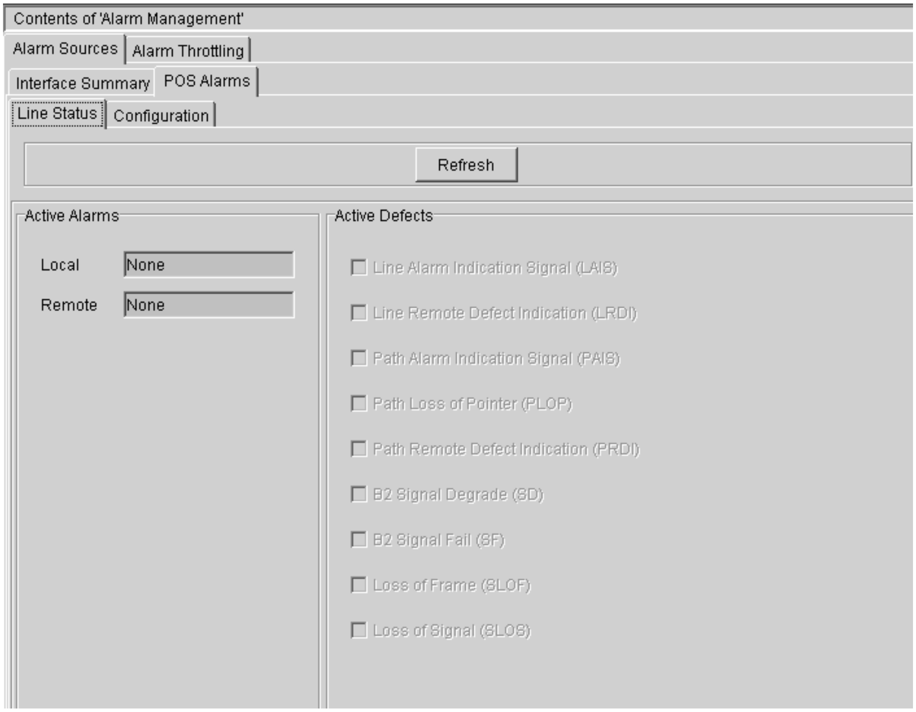
Viewing Line Status

To view the alarms and defects currently reported on a POS interface, follow this procedure:

1. In the Interface Summary window, select the row that includes the POS interface. The POS interface is identified by the slot in which the POS module is installed.
2. Click the **POS Alarms** tab.
3. Click the **Line Status** tab.
4. Click **Refresh** to update the information.

What You See

Figure 11-8 Line Status window.



Active Alarms

Local: None

Remote: None

Active Defects

□ Line Alarm Indication Signal (LAIS)

□ Line Remote Defect Indication (LRDI)

□ Path Alarm Indication Signal (PAIS)

□ Path Loss of Pointer (PLOP)

□ Path Remote Defect Indication (PRDI)

□ B2 Signal Degrade (SD)

□ B2 Signal Fail (SF)

□ Loss of Frame (SLOF)

□ Loss of Signal (SLOS)

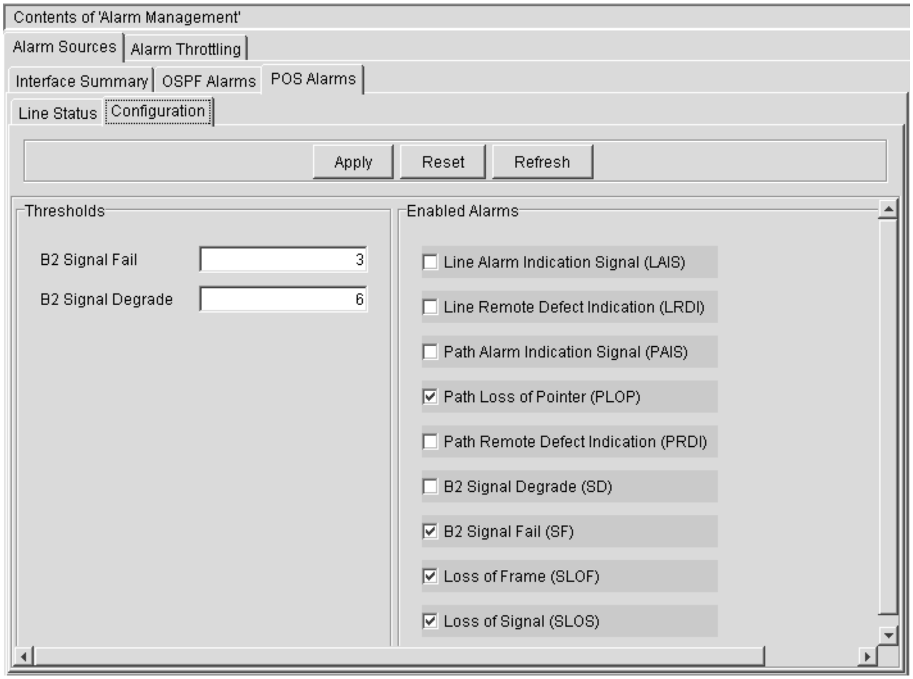
Configuring POS Alarms

To configure the alarms and defects that you want the selected POS interface to report, follow this procedure:

1. In the Interface Summary window, select the POS interface that you wish to configure.
2. Click the **POS Alarms** tab.
3. Click the **Configuration** tab.
4. Choose the alarms options that you wish the selected POS interface to report.
5. Click **Apply** to commit the information or click **Reset** to return to the previous values.

What You See

Figure 11-9 POS Alarms Configuration Window



B2 Signal Fail 3

B2 Signal Degrade 6

- ☐ Line Alarm Indication Signal (LAIS)
- ☐ Line Remote Defect Indication (LRDI)
- ☐ Path Alarm Indication Signal (PAIS)
- ☑ Path Loss of Pointer (PLOP)
- ☐ Path Remote Defect Indication (PRDI)
- ☐ B2 Signal Degrade (SD)
- ☑ B2 Signal Fail (SF)
- ☑ Loss of Frame (SLOF)
- ☑ Loss of Signal (SLOS)

For details, see Chapter 10, "Packet Over SONET Administration".

Parameter Descriptions

This table provides a description of the POS Alarms Configuration window alarms.

Table 11-3 POS Configuration Parameters

Alarm	Description
Line Alarm Indication Signal (LAIS)	Disabled by default, configures the interface to report line alarm indication signal errors.
Line Remote Defect Indication (LRDI)	Disabled by default, configures the interface to report line remote defect indication errors.

Alarm	Description
Path Alarm Indication Signal (PAIS)	Disabled by default, configures the system to report path alarm indication signal errors. Line terminating equipment (LTE) send packet alarm indication signals to alert downstream path terminating equipment (PTE) of defects on their incoming line signal.
Path Loss of Pointer (PLOP)	Enabled by default, configures the interface to report path loss of pointer errors. A PLOP error may result from an invalid pointer or too many new data flag enabled indications.
Path Remote Defect Indication (PRDI)	Disabled by default, configures the interface to report path remote defect indication errors.
B2 Signal Degrade (SD)	Disabled by default, configures the interface to report when the B2 signal degrades enough to meet or cross a specified Bit Error Rate (BER) threshold. Specify this threshold in the B2 Signal Degrade field on the left of the screen. The default BER threshold for B2 signal failure is 6.
B2 Signal Fail (SF)	Enabled by default, configures the interface to report a failure when the B2 signal degrades enough to meet or cross a specified Bit Error Rate (BER) threshold. Specify this threshold in the B2 Signal Fail field on the left of the screen. The default BER threshold for B2 signal failure is 3.
Loss of Frame (SLOF)	Enabled by default, configures the interface to report section loss of frame errors. The interface detects SLOF when an error on the incoming SONET signal persists for at least 3 milliseconds.
Loss of Signal (SLOS)	Enabled by default, configures the interface to report loss of signal (SLOS) errors. The POS interface reports a SLOS error under either of the following conditions: When an all-zeros pattern on the incoming SONET signal lasts at least 19(+-3) microseconds. If the signal level drops below the a specified threshold.

Alarm Throttling

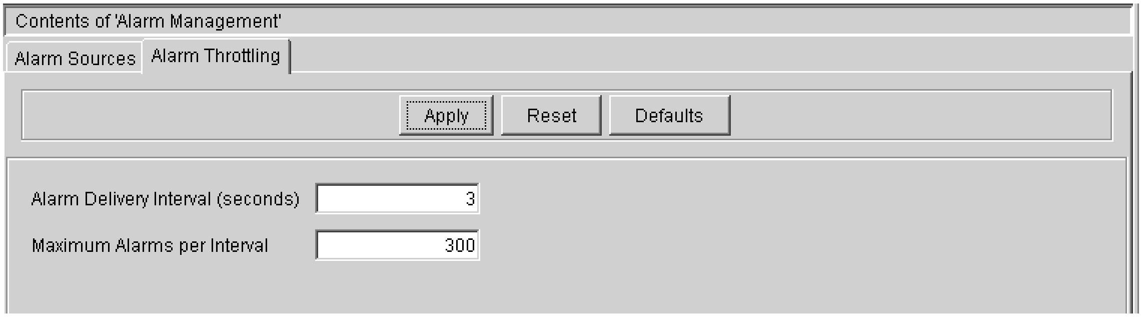
Alarm throttling allows you to specify a maximum number of Traps that the system can send to the table within a given time interval. The alarm throttling value that you configure applies only to the Traps displayed by the Alarm Table, not to the number of Traps sent to the alarm log.

To configure alarm throttling, use this procedure:

1. In the Alarm Management window, click the **Alarm Log Throttling** tab.
2. Enter values for the parameters: Refer to Table 11-4.
3. Perform one of these tasks:
   - Click **Apply** to commit the information
   - Click **Reset** to return to the previous values.
   - Click **Defaults** to return to the default values.

What You See

Figure 11-10 Alarm Throttling Window



Contents of 'Alarm Management'

Alarm Delivery Interval (seconds) 3

Maximum Alarms per Interval 300

Parameter Descriptions

This table provides a description of the Alarm Throttling window.

Table 11-4 Alarm Throttling Parameters.

Parameter	Description
Alarm Delivery Interval	Interval during which the system transmits Trap notifications. By default, the Alarm Delivery Interval is set to 3 seconds.
Maximum Alarms per Interval	Maximum number of Traps that the system can transmit during the specified alarm delivery interval. By default the Maximum Alarms per Interval is set to 300. This means that the system can generate a maximum of 300 Traps every 3 seconds

Configuring Hardware Alarms

This section provides information about the monitoring and reporting of hardware alarms and includes:

- DB15 Alarms
- Fan Assertion Levels
- Power Supply Assertion Levels

The Cuda 12000 utilizes an external fan tray for cooling and obtains power from an external power source. Fault management and reporting features on the Cuda 12000 allow you to configure the reporting of fault conditions as they arise on these critical devices so you may take action prior to a loss of operation, or know when the power source and cooling capability is compromised.

For a single chassis, you can connect these external components:

- **Fan Tray** — The ADC-provided fan tray is a required component and serves as the system cooling unit.
- **Power Supply A** — A single -48 volt DC power source is required for system operation.
- **Power Supply B** — Connection to a second power source is optional to provide redundancy.

For more information about the Cuda 12000 cooling and power features, see the "Cuda 12000 IP Access Switch Installation Guide."

Two DB-15 connectors—*alarms in* and *alarms out*—on the rear of the chassis enable communication of alarms from external power and fan units. Using a ADC-provided cable, you connect the *alarms-in* connector to the external fan tray and power supplies that you want to monitor. The external devices then transmit alarms into the chassis over this connection. The other DB-15 is the *alarms out* connection used to connect an external alarm indication device.

For information about how to cable the fan tray and power supplies to the chassis for fault reporting, see the Cuda 12000 IP Access Switch Installation Guide.

Before You Begin

Before you begin to configure the hardware alarms, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **Fault Management** > **Aux Devices.**
2. Click the **Hardware Alarm Configuration** tab. The Hardware Alarm Configuration window appears.

Configuring Alarms Out

A DB-15 connector on the Cuda 12000 chassis rear panel serves as the *alarms out* port. You can configure the system to send specific types of alarm signals out this DB-15 connector to the LED display to notify a device that a particular type of fault has occurred. Each fault can generate one or more types of alarm signals.

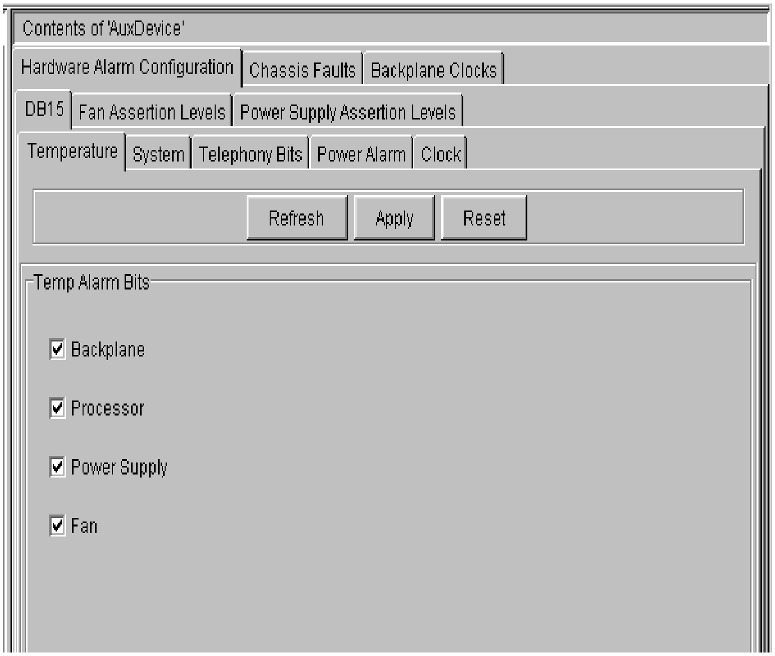
To configure the alarm bits, follow this procedure:

1. In the Hardware Alarm Configuration window, click the **DB15** tab.
2. Click one of the DB15 tabs. The options are:
   - Temperature
   - System
   - Telephony Bits
   - Power Alarm
   - Clock
3. Select the temperature alarm bits that you wish to trigger. When the check box is clear, no alarm is reported to the external device. The check box is clear by default.

   If you select the check box, an alarm is reported to the external indication device. This could be an audible alarm or LED display.
4. Click **Apply** to commit the information or click **Reset** to return to the default values.
5. Click **Refresh** to update the information.

What You See

Figure 11-11 DB15 Window



Temp Alarm Bits

☑ Backplane

☑ Processor

☑ Power Supply

☑ Fan

Parameter Descriptions

This table provides a description of the DB15 alarm options.

This Signal:	Provides Notification of These Faults:
Temperature	■ Backplane ■ Processor ■ Power Supply ■ Fan

This Signal:	**Provides Notification of These Faults:**
System	■ Backplane
	■ Backplane Temperature
	■ Backplane Power
	■ Backplane Power A
	■ Backplane Power B
	■ Red Alarm
	■ Power Supply Temperature
	■ Power Supply AC
	■ Power Supply DC
	■ Fan Temperature
	■ Fan Rotation
Telephony Bits	
Red Alarm Fault Bits	■ Bits A
	■ Bits B
	■ Red Alarm
Blue Alarm Bits	■ Blue
Yellow Alarm Bits	■ Yellow
Power Alarm	
Power Alarm Bits	■ Local Power A
	■ Local Power B
	■ Backplane Power
	■ Backplane Power A
	■ Backplane Power B
	■ Power Supply AC
	■ Power Supply DC
Power A Fail Bit	■ Power Fail A
Power B Fail Bit	■ Power Fail B

This Signal:	Provides Notification of These Faults:
Clock	■ Bits A ■ Bits B ■ Red Alarm

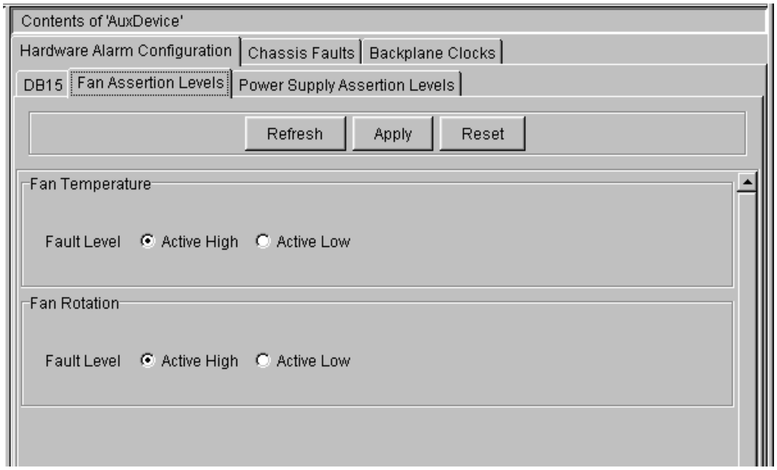
Configuring Fan Unit Assertion Levels

The ADC-provided fan unit utilizes an active low signal to inform the management module of system faults, so ensure that the assertion level for fan temperature and fan rotation faults is set to *active low*. To set the assertion level logic used by the fan tray unit to report temperature and rotation faults, follow this procedure:

1. In the Hardware Alarm Configuration window, click the **Fan Supply Assertion Levels** tab.
2. Select the proper fault level for the Fan Temperature and Fan Rotation. The signal that the device sends can use one of these assertion levels:
   - Active High — Signal indicates the assertion state as a logic ONE state.
   - Active Low — Signal indicates the assertion state as a logic ZERO state.
3. Click **Apply** to commit the changes or click **Reset** to exit without saving.
4. Click **Refresh** to update the information.

What You See

Figure 11-12 Fan Supply Assertion Levels Window



Fan Temperature

Fault Level ● Active High ○ Active Low

Fan Rotation

Fault Level ● Active High ○ Active Low

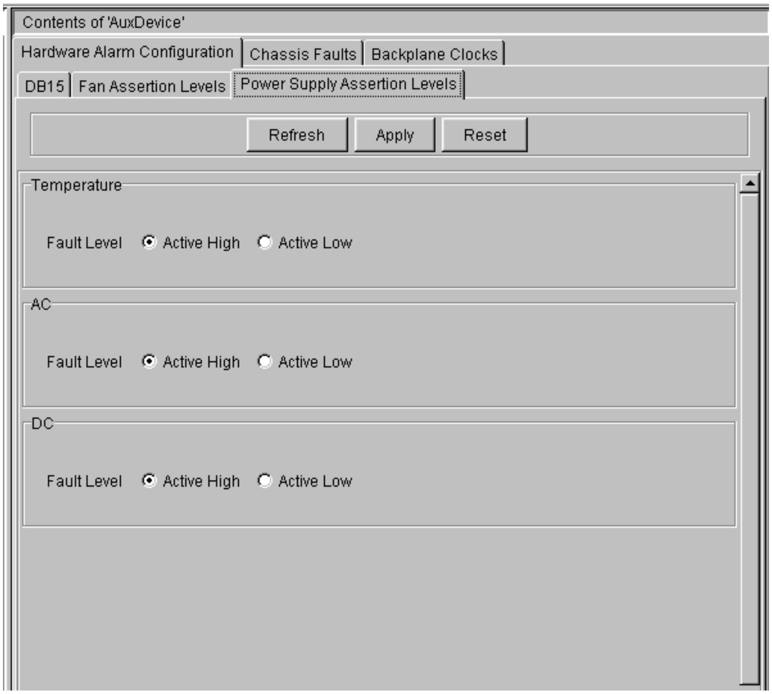
Configuring the Power Assertion Level

You must configure the assertion level that the attached devices use when indicating a fault condition. You must verify the assertion level used by the attached power supplies and set the AC-monitor, DC-monitor, and power supply temperature assertion levels accordingly. To set the power assertion levels, follow this procedure:

1. In the Hardware Alarm Configuration window, click the **Power Supply Assertion Levels** tab.
2. Select the proper fault level for the Temp, AC, and DC options. The signal that the device sends can use one of these assertion levels:
   - Active High — Signal indicates the assertion state as a logic ONE state.
   - Active Low — Signal indicates the assertion state as a logic ZERO state.
3. Click **Apply** to commit the changes or click **Reset** to exit without saving.
4. Click **Refresh** to update the information.

What You See

Figure 11-13 Power Supply Assertion Levels Window



Temperature

Fault Level ● Active High ○ Active Low

AC

Fault Level ● Active High ○ Active Low

DC

Fault Level ● Active High ○ Active Low

Configuring Fault Reporting

The system reports faults in the form of SNMP notifications. You must select the faults for which you want to be notified. For each fault that you choose to report, the system sends an SNMP trap to all destinations in the system's Trap destination table. Traps are only sent when there is a state transition from *okay* to *faulted* or a transition from *faulted* to *okay*. To configure SNMP notifications, see, Chapter 7, "Simple Network Management Protocol (SNMP)".

Before You Begin

Before you begin, follow this procedure:

1. navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Fault Management** > **Aux Devices.**
2. Click the **Chassis Faults** tab. The resulting window appears.

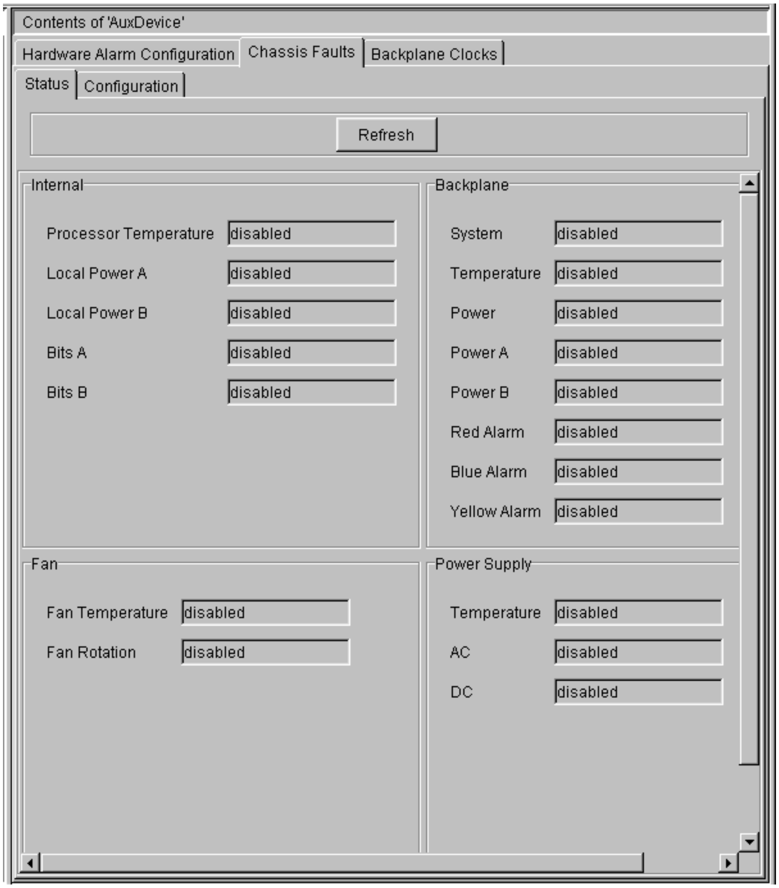
Viewing the State of Fault Conditions

To display the state of each fault condition, follow this procedure:

1. In the **Chassis Faults** window, click the **Status** tab. Each fault displays one of these states:
   - disabled — Reporting is turned off for the fault condition. An SNMP Trap or syslog message is not generated should the fault condition occur. This is the default status.
   - okay — Fault reporting is enabled. The fault condition has not occurred; or, the fault condition occurred, has been corrected and is now okay.
   - faulted — Fault reporting is enabled; an SNMP Trap or syslog message is generated when the fault condition occurs.
2. Click **Refresh** to update the information.

What You See

Figure 11-14 Chassis Faults Status Window.



Internal

Processor Temperature	disabled
Local Power A	disabled
Local Power B	disabled
Bits A	disabled
Bits B	disabled

Backplane

System	disabled
Temperature	disabled
Power	disabled
Power A	disabled
Power B	disabled
Red Alarm	disabled
Blue Alarm	disabled
Yellow Alarm	disabled

Fan

Fan Temperature	disabled
Fan Rotation	disabled

Power Supply

Temperature	disabled
AC	disabled
DC	disabled

Configuring for Reporting Chassis Faults

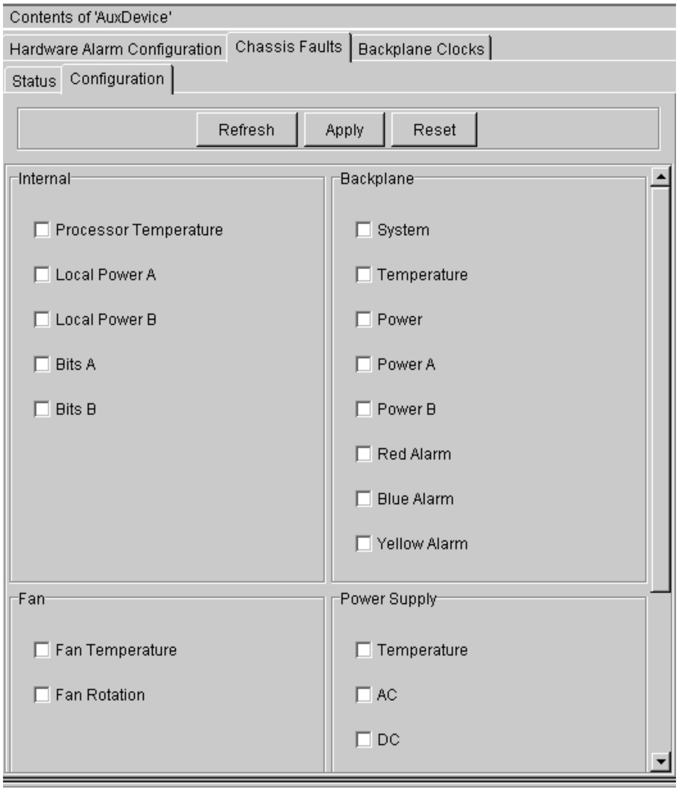
To configure fault reporting, follow this procedure:

1. In the **Chassis Faults** window, click the **Configuration** tab.
2. Select the faults that you wish to report. Selecting the check box indicates you wish to have reporting for that notification. Clearing the check box indicates no reporting.

3. Click **Apply** to commit the changes or click **Reset** to exit without saving.
4. Click **Refresh** to update the information.

What You See

Figure 11-15 Chassis Faults Configuration Window



Internal

□ Processor Temperature
□ Local Power A
□ Local Power B
□ Bits A
□ Bits B

Backplane

□ System
□ Temperature
□ Power
□ Power A
□ Power B
□ Red Alarm
□ Blue Alarm
□ Yellow Alarm

Fan

□ Fan Temperature
□ Fan Rotation

Power Supply

□ Temperature
□ AC
□ DC

Parameter Descriptions

This table provides a description of the Chassis Faults Configuration parameters.

Table 11-5 Chassis Faults Configuration Parameters

Fault	Description
Backplane	

Fault	Description
System	A payload blade asserted a backplane system fault condition.
Temperature	One or more payload blades detected a Temperature Fault.
Power	One or more payload blades detected an internal Power Fault.
Power A	One or more payload blades detected a Power_A (48V) Fault or switch A is disabled.
Power B	One or more payload blades detected a Power_B (48V) Fault or switch B is disabled.
Red Alarm	One or more payload blades has asserted a Red Alarm.
Blue Alarm	One or more payload blades has asserted a Blue Alarm.
Yellow Alarm	One or more payload blades has asserted a Yellow Alarm.
Power Supply	
Temperature	One or more payload blades detected a Temperature Fault.
AC	The power supply associated with the chassis detected the loss of one or more AC inputs.
DC	The power supply associated with the chassis detected a DC out-of-range fault.
Internal	
Processor Temperature	The chassis manager associated with the chassis detected a processor over-temperature condition.
Local Power A	The chassis manager associated with the chassis detected a loss of Power_A (48V) on a module.
Local Power B	The chassis manager associated with the chassis detected a loss of Power_B (48V) to the chassis.
Bits A	The chassis manager associated with the chassis detected a loss of the BITS-A clock to the chassis.
Bits B	The chassis manager associated with the chassis detected a loss of the BITS-B clock.
Fan	
Fan Temperature	The fan tray associated with the chassis detected an inlet temperature > 50°C.
Fan Rotation	The fan tray associated with the chassis detected one or more non-rotating fans.

Configuring for Backplane Clock Sources

The Cuda 12000 IP Access Switch backplane has a primary clock (A) and a secondary clock (B). For each of these clocks, you can configure one of the following clock sources:

- External BITS-A clock source
- External BITS-B clock source
- External Packet-Over-SONET (POS) clock source
- Internal Stratum-3 oscillator clock source on the management module

If you do not configure any clock sources, each DOCSIS/EuroDOCSIS module uses its own clock.

If you are using a BITS-A or BITS-B external clock source, make sure that the Cuda 12000 is connected to the appropriate clock sources via the BITS-A or BITS-B external clock connectors. Refer to the *Cuda 12000 IP Access Switch Installation Guide* for more information on these connectors.

If you are using a POS module as the clock source, make sure that the interface on the POS module has been configured to receive clocking from the other (remote) side of the POS link. Refer to Chapter 10, "Packet Over SONET Administration", for more information on configuring POS interfaces.

A typical configuration would be as follows:

- Primary clock configured to use a BITS-A or BITS-B external clock source
- Secondary clock configured to use the internal Stratum-3 oscillator clock source.

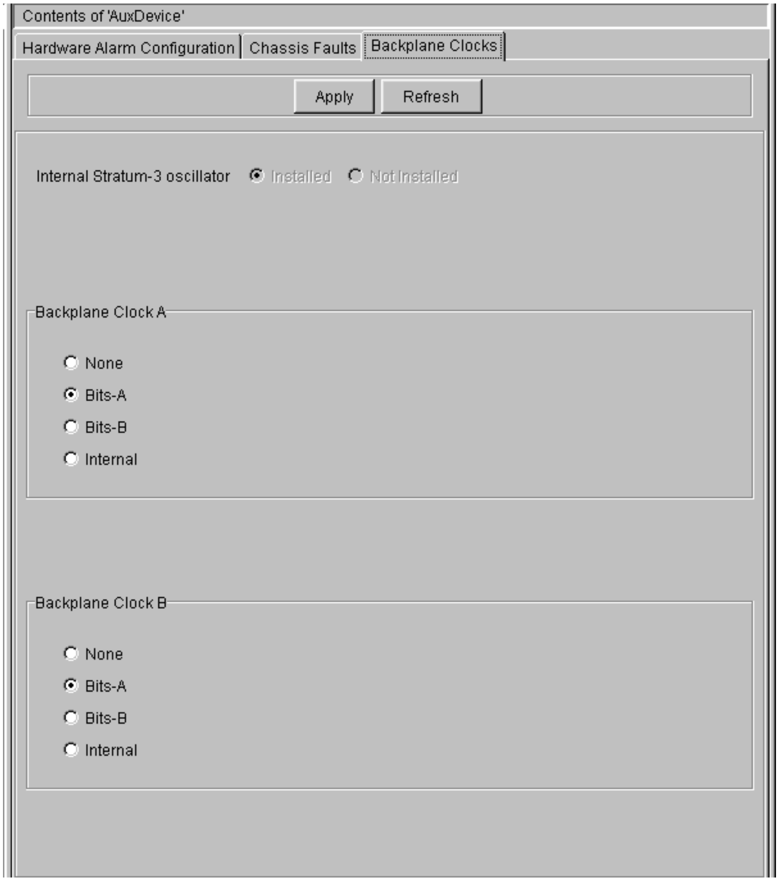
Before You Begin

Before you begin, follow this procedure:

1. navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Fault Management** > **Aux Devices.**
2. Click the Backplane Clocks tab.

What You See

Figure 11-16 Backplane Clocks Window



Internal Stratum-3 oscillator ● Installed ○ Not Installed

Backplane Clock A

○ None
● Bits-A
○ Bits-B
○ Internal

Backplane Clock B

○ None
● Bits-A
○ Bits-B
○ Internal

Parameter Descriptions

This table provides a description of the backplane clock configuration parameters:

Table 11-6 Backplane Clock Configuration Parameters

Parameter	Description
Internal Stratum-3 oscillator	Used to drive either backplane clock.

Parameter	**Description**
Installed	Means that Stratum clock is installed. Required for supporting backplane clocks.
Not installed	Means that stratum clock is not installed. Backplane clocks are not supported on the chassis.
Backplane Clock A	Used to specify which clock source is driven onto the primary clock.
None	Not driven by any clock.
Bits A	Driven by external clock bits A.
Bits B	Driven by external clock bits B.
Internal	Driven by Internal Stratum-3 oscillator
Backplane Clock B	Used to specify which clock source is driven onto the secondary backplane clock B.
None	Not driven by any clock.
Bits A	Driven by external clock bits A.
Bits B	Driven by external clock bits B.
Internal	Driven by Internal Stratum-3 oscillator

III

IP ROUTING

12 CONFIGURING IP ROUTING

The Cuda 12000 uses the Internet Protocol (IP) to exchange data over computer networks. In addition, the Cuda 12000 supports RIP and OSPF routing protocols to exchange routing information with other routers in the IP network.

Configuring IP Routing consists of the following tasks:

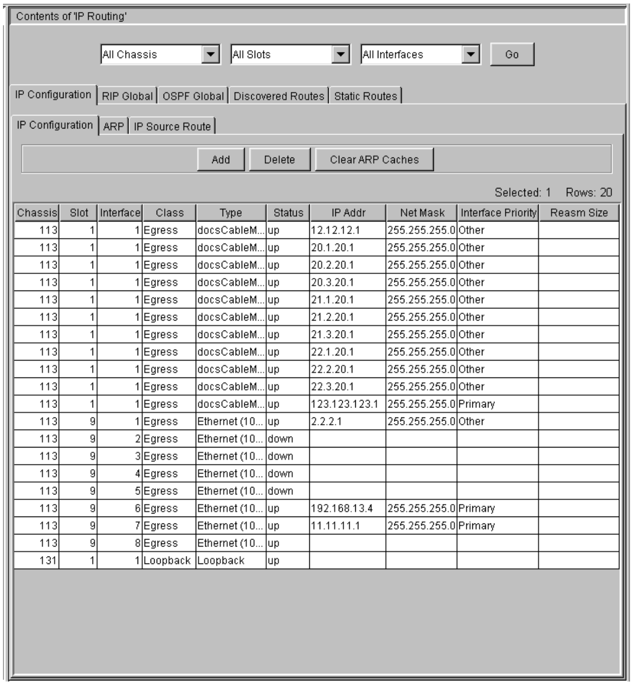
- Configuring IP
- Configuring ARP Entries
- Configuring Source Routing
- Configuring RIP Global
- Configuring OSPF Global
- Configuring OSPF Interfaces
- Configuring OSPF Virtual Interfaces
- Viewing Discovered Routes
- Configuring Static Routes

For information about Import and Export Route Filtering, refer to Chapter 13, "Creating Route Filters", on page 359.

Before You Begin

This sections describes the functions involved with the IP Routing configuration window. To access the IP Routing window, navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **IP** > **IP Routing**. The IP Routing window opens as shown in the next figure.

Figure 12-1 IP Routing Window



Selected: 1 Rows: 20

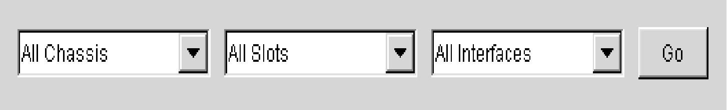
Chassis	Slot	Interface	Class	Type	Status	IP Addr	Net Mask	Interface Priority	Reasm Size
113	1	1	Egress	docsCableM...	up	12.12.12.1	255.255.255.0	Other	
113	1	1	Egress	docsCableM...	up	20.1.20.1	255.255.255.0	Other	
113	1	1	Egress	docsCableM...	up	20.2.20.1	255.255.255.0	Other	
113	1	1	Egress	docsCableM...	up	20.3.20.1	255.255.255.0	Other	
113	1	1	Egress	docsCableM...	up	21.1.20.1	255.255.255.0	Other	
113	1	1	Egress	docsCableM...	up	21.2.20.1	255.255.255.0	Other	
113	1	1	Egress	docsCableM...	up	21.3.20.1	255.255.255.0	Other	
113	1	1	Egress	docsCableM...	up	22.1.20.1	255.255.255.0	Other	
113	1	1	Egress	docsCableM...	up	22.2.20.1	255.255.255.0	Other	
113	1	1	Egress	docsCableM...	up	22.3.20.1	255.255.255.0	Other	
113	1	1	Egress	docsCableM...	up	123.123.123.1	255.255.255.0	Primary	
113	9	1	Egress	Ethernet (10...	up	2.2.2.1	255.255.255.0	Other	
113	9	2	Egress	Ethernet (10...	down				
113	9	3	Egress	Ethernet (10...	down				
113	9	4	Egress	Ethernet (10...	down				
113	9	5	Egress	Ethernet (10...	down				
113	9	6	Egress	Ethernet (10...	up	192.168.13.4	255.255.255.0	Primary	
113	9	7	Egress	Ethernet (10...	up	11.11.11.1	255.255.255.0	Primary	
113	9	8	Egress	Ethernet (10...	up				
131	1	1	Loopback	Loopback	up				

Chassis/Slot/Interface Heading Panel

For all IP Routing windows, a heading panel appears and provides the relevant chassis, slot, and interface information. The heading panel acts as a filtering table that offers you the ability to filter specific chassis/slot/interface views, in addition to looking at the entire table. This allows you to restrict the window display, which makes it is easier and quicker to read the table and manage configuration.

Once you select the chassis/slot/interface that you wish to configure or view, click **Go**.

Figure 12-2 Chassis/Slot/Interface Heading Panel



Configuring IP

IP (Internet Protocol) configuration provides interconnectivity of networks. It provides a means for which hosts and routers process transmitted or received packets, and determines when an error should be generated and IP packets discarded. IP configuration also supports a loopback interface.

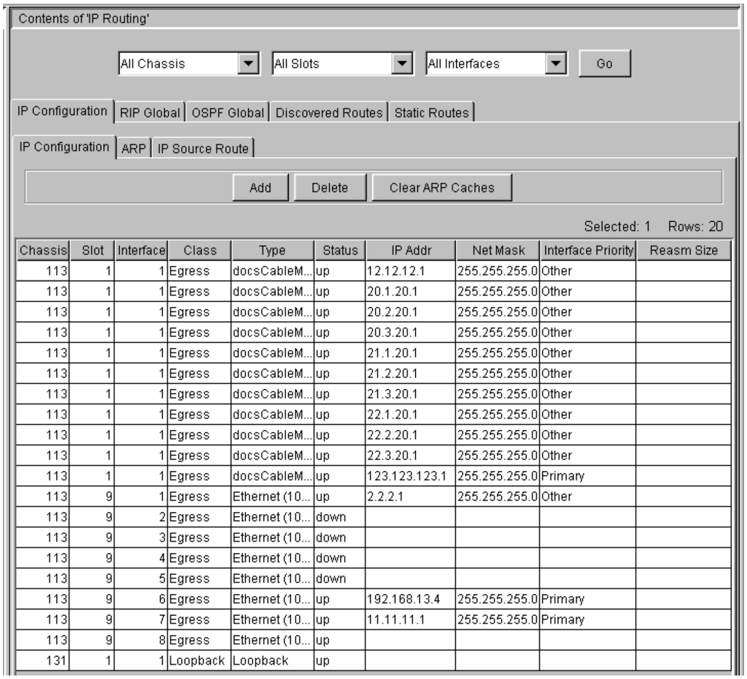
Configuring IP involves adding IP Interfaces and Static ARP addresses (Address Resolution Protocol), and configuring a loopback interface.

Before You Begin

To view the current IP configuration, follow this procedure:

1. Navigate to **Network Browser**> GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **IP** > **IP Routing**.
2. In the IP Routing window, click **IP Configuration** tab.
3. Click the **IP Configuration** sub tab. The IP Configuration window appears as shown in the figure below

Figure 12-3 IP Configuration Window.



Selected: 1 Rows: 20

Chassis	Slot	Interface	Class	Type	Status	IP Addr	Net Mask	Interface Priority	Reasm Size
113	1	1	Egress	docsCableM...	up	12.12.12.1	255.255.255.0	Other	
113	1	1	Egress	docsCableM...	up	20.1.20.1	255.255.255.0	Other	
113	1	1	Egress	docsCableM...	up	20.2.20.1	255.255.255.0	Other	
113	1	1	Egress	docsCableM...	up	20.3.20.1	255.255.255.0	Other	
113	1	1	Egress	docsCableM...	up	21.1.20.1	255.255.255.0	Other	
113	1	1	Egress	docsCableM...	up	21.2.20.1	255.255.255.0	Other	
113	1	1	Egress	docsCableM...	up	21.3.20.1	255.255.255.0	Other	
113	1	1	Egress	docsCableM...	up	22.1.20.1	255.255.255.0	Other	
113	1	1	Egress	docsCableM...	up	22.2.20.1	255.255.255.0	Other	
113	1	1	Egress	docsCableM...	up	22.3.20.1	255.255.255.0	Other	
113	1	1	Egress	docsCableM...	up	123.123.123.1	255.255.255.0	Primary	
113	9	1	Egress	Ethernet (10...	up	2.2.2.1	255.255.255.0	Other	
113	9	2	Egress	Ethernet (10...	down				
113	9	3	Egress	Ethernet (10...	down				
113	9	4	Egress	Ethernet (10...	down				
113	9	5	Egress	Ethernet (10...	down				
113	9	6	Egress	Ethernet (10...	up	192.168.13.4	255.255.255.0	Primary	
113	9	7	Egress	Ethernet (10...	up	11.11.11.1	255.255.255.0	Primary	
113	9	8	Egress	Ethernet (10...	up				
131	1	1	Loopback	Loopback	up				

4. Select the chassis, slot, and interface that you wish to access.

Parameter Descriptions

This table provides a description of the IP Configuration window

Table 12-1 IP Configuration Window Parameter Descriptions

Parameter	Description
Chassis	Number that you assign to the chassis in the network.
Slot	Physical slot in which the interface module is installed.
Interface	Number of the physical interface on the interface module.
Class	Indicates that the interface is Egress.
Type	Indicates the interface type. The Cuda 12000 supports the these types: CMTS: includes the docsCableMAClayer MIB object. Ethernet: includes the 10 Mb, 100 Mb, or Gigabit interfaces. POS: Includes the OC-3 and OC-12 interfaces.
Status	Indicates whether the interface is up (in service) or down (not in service).

Parameter	Description
IP Addr	IP address for this interface
Net Mask	Network mask for this interface.
Interface Priority	Specifies the priority of the source IP address for sending packets originating at the interface.
Reasm Size	Largest IP datagram that the router can reassemble from incoming IP fragmented datagrams received on the interface.

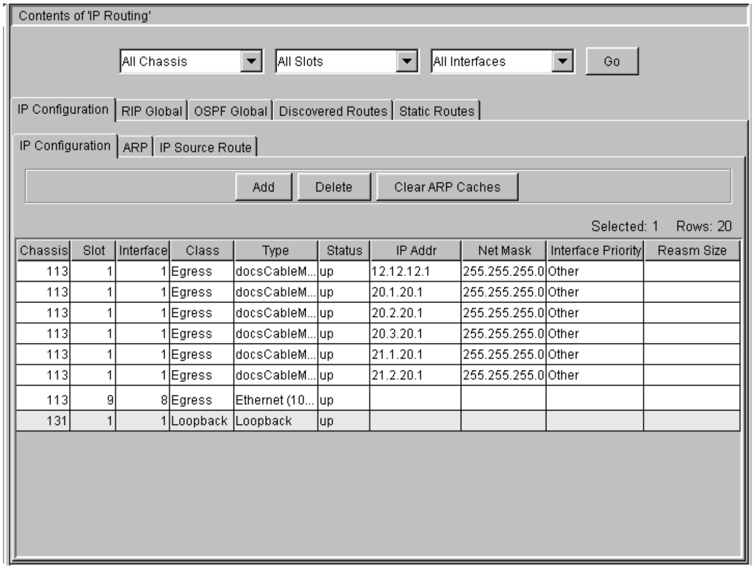
Loopback Interface

A router can relay traffic to the management module through any of the IP interfaces or through loopback. A loopback interface is a logical interface that is designated as 131/1/1 and appears in the list of IP interfaces within the IP Configuration main panel.

If you select the loopback interface as the interface to which you are adding an IP address, a router is able to forward traffic through loopback if the interface designated by the IP address goes down. You can only add or delete IP addresses associated with the Loopback Interface; no other functions are enabled (other tabs and the **Clear ARP Caches** button remain disabled.

What You See

Figure 12-4 Loopback Interface Selected



Selected: 1 Rows: 20

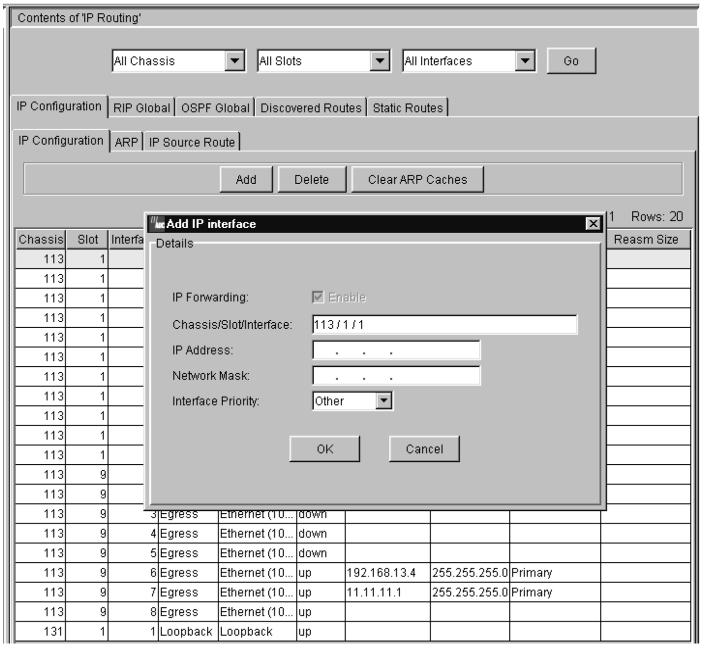
Chassis	Slot	Interface	Class	Type	Status	IP Addr	Net Mask	Interface Priority	Reasm Size
113	1	1	Egress	docsCableM...	up	12.12.12.1	255.255.255.0	Other	
113	1	1	Egress	docsCableM...	up	20.1.20.1	255.255.255.0	Other	
113	1	1	Egress	docsCableM...	up	20.2.20.1	255.255.255.0	Other	
113	1	1	Egress	docsCableM...	up	20.3.20.1	255.255.255.0	Other	
113	1	1	Egress	docsCableM...	up	21.1.20.1	255.255.255.0	Other	
113	1	1	Egress	docsCableM...	up	21.2.20.1	255.255.255.0	Other	
113	9	8	Egress	Ethernet (10...	up				
131	1	1	Loopback	Loopback	up				

Adding an IP Interface

IP Interfaces refer to the IP addresses that are assigned to all network interfaces over which you intend to connect to your IP network. To add an IP address follow this procedure:

1. In the **IP Configuration** window, select the interface on which you want to add the IP address.
2. Click **Add.** The Add IP Interface window appears as shown in the next figure.

Figure 12-5 Add IP Interface Window



IP Forwarding: ☑ Enable

Chassis/Slot/Interface: 113 / 1 / 1

IP Address: . . .

Network Mask: . . .

Interface Priority: Other

Chassis	Slot	Interfa							Reasm Size
113	1								
113	1								
113	1								
113	1								
113	1								
113	1								
113	1								
113	1								
113	1								
113	1								
113	1								
113	9								
113	9								
113	9	3	Egress	Ethernet (10...	down				
113	9	4	Egress	Ethernet (10...	down				
113	9	5	Egress	Ethernet (10...	down				
113	9	6	Egress	Ethernet (10...	up	192.168.13.4	255.255.255.0	Primary	
113	9	7	Egress	Ethernet (10...	up	11.11.11.1	255.255.255.0	Primary	
113	9	8	Egress	Ethernet (10...	up				
131	1	1	Loopback	Loopback	up				

3. Enter values for the parameters. Refer to Table 12-2.
4. Click **OK** to commit the changes or click **Cancel** to exit without saving.

Parameter Descriptions

This table provides a description of the Add IP Interface window

Table 12-2 .Add IP Interface Window Parameters

Parameter	Description
IP Forwarding	By default, IP Forwarding is Enabled for the interface.
Chassis/Slot/Interface	Indicates the chassis, slot, and interface for which you wish to add an IP interface.
IP Address	Source IP address for packets originating at the interface.
Network Mask	Network mask for this interface.

Parameter	Description
Interface Priority	Specifies the priority of the source IP address for sending packets originating at the interface. Select the preference for this IP address relative to other IP addresses on the interface. The options are Primary, Secondary, or Other. For example, if you wish the source IP address for ICMP redirect to use this IP address, select Primary. If you wish to use a different IP address, then select Secondary. If you do not have a preference, select Other.

Deleting IP Interfaces

Deleting an IP Interface involves removing the selected IP Address from the selected interface. For example, all logical interfaces that associate with it, such as RIP and OSPF interfaces, are deleted. To delete an IP interface, follow this procedure:

1. In the **IP Configuration** window, select the interface you wish to delete.
2. Click **Delete.** A confirmation window appears.
3. Click **Yes** to continue or click **Cancel** to cancel the deletion.

Configuring ARP Entries

ARP (Address Resolution Protocol) maps the MAC layer addressing with the IP layer addressing on a physical network that allows multiple access (such as for Ethernet).

Each host on an IP network has two addresses:

- MAC address, identifies the host at layer 2 in the data link layer of the OSI model.
- IP address, identifies the host at layer 3 of the OSI model and indicates the network to which it belongs.

To communicate with a host on an IP network, an interface must know the MAC address and IP address of the target host. The interface can learn the MAC address (or physical address) from the network address using ARP.

You cannot add ARP entries to CMTS interfaces because the SID information is unknown. See section below, “Enable Simple Proxy ARP,” for further information about CMTS interfaces.

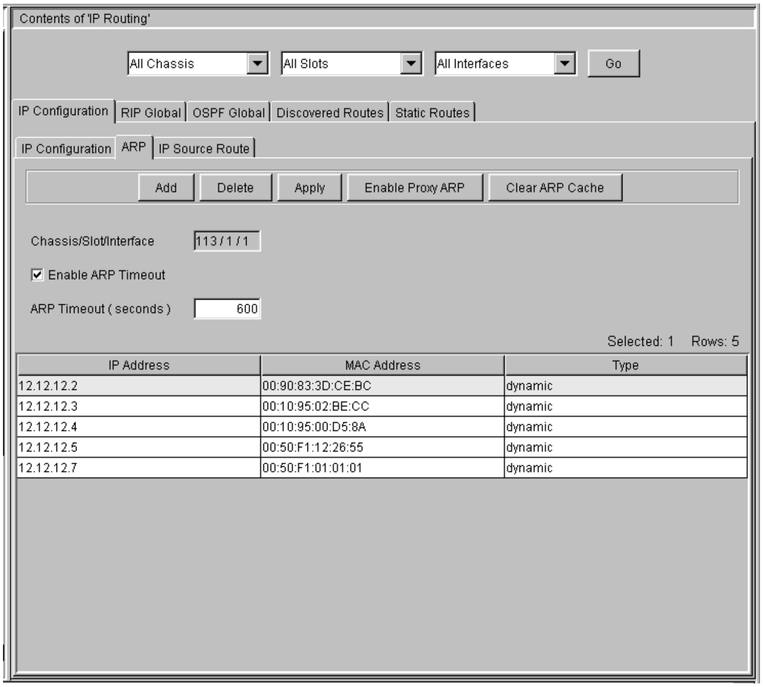
Before You Begin

The ARP window displays the MAC-IP address mappings that the system learns (dynamic addresses) and the manually added APR entries. To view the current ARP entries, follow this procedure:

1. In the IP Routing window, click **IP Configuration** tab.
2. Click the **IP Configuration** sub tab.
3. Select the row that includes the interface on which you want to add an IP source route.
4. Click the **ARP** tab. The ARP window appears.

What You See

Figure 12-6 IP Configuration ARP Window



Chassis/Slot/Interface 113 / 1 / 1

☑ Enable ARP Timeout

ARP Timeout (seconds) 600

Selected: 1 Rows: 5

IP Address	MAC Address	Type
12.12.12.2	00:90:83:3D:CE:BC	dynamic
12.12.12.3	00:10:95:02:BE:CC	dynamic
12.12.12.4	00:10:95:00:D5:8A	dynamic
12.12.12.5	00:50:F1:12:26:55	dynamic
12.12.12.7	00:50:F1:01:01:01	dynamic

Parameter Descriptions

This table provides a description of the IP Configuration ARP window.

Table 12-3 ARP Window Parameters

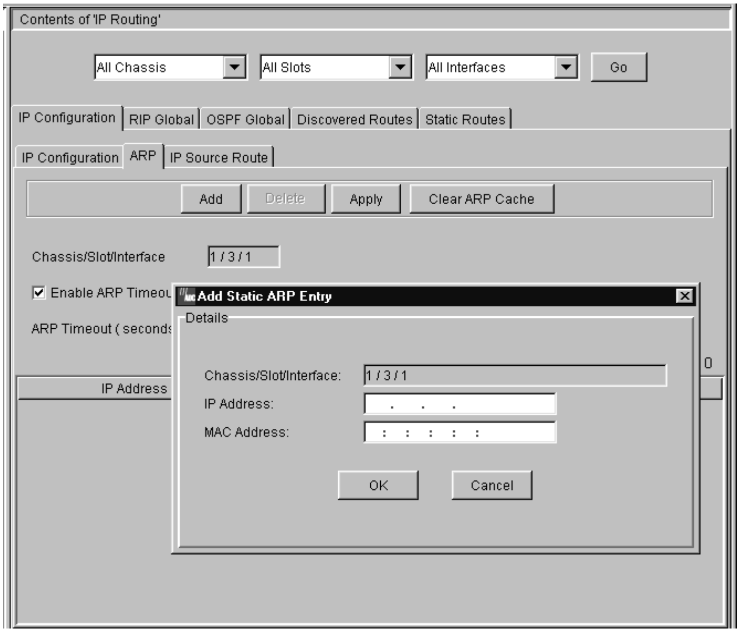
Parameter	Description
Chassis/Slot/Interface	Indicates the chassis, slot, and interface for which you wish to add an IP interface.
Enable ARP Timeout	Checking the box enables ARP cache entries for which there have been no traffic to timeout. Clearing the box disables timeout.
ARP Timeout (seconds)	Timeout interval for ARP cache entries. The default value is 600 seconds.
IP Address	Source IP address for packets originating at the interface.
MAC Address	MAC address of the attached device.
Type	Indicates if the ARP entry is dynamic or static.

Adding an ARP Map Entry

To add an ARP Map entry, follow this procedure.

1. In the **IP Configuration** window, select the row that includes the interface on which you want to add an IP source route.
2. Click the **ARP** tab.
3. Select the chassis, slot, and interface that you wish to access.
4. Click **Add.** The Add Static ARP Entry window opens as shown in the next figure.

Figure 12-7 Add Static ARP Entry Window



Contents of 'IP Routing'

All Chassis / All Slots / All Interfaces

Chassis/Slot/Interface 1 / 3 / 1

☑ Enable ARP Timeou

ARP Timeout (seconds

Add Static ARP Entry

Details

Chassis/Slot/Interface: 1 / 3 / 1

IP Address: . . .

MAC Address: : : : : :

5. Enter the IP and MAC addresses that you wish to use for the mapping.
6. Click **OK** to commit the information or click **Cancel** to exit without saving.
7. Click **Apply** to commit the changes.

Deleting an ARP Entry

Deleting ARP removes the bind between the MAC and IP address layers of a specified interface. To delete an ARP entry, follow this procedure:

1. In the **IP Configuration** window, select the row that includes the interface on which you want to add an IP source route.
2. Click the **ARP** tab.
3. Click **Delete**. A confirmation window appears.
4. Click **Yes** to continue or click **No** to cancel the deletion.
5. Click **Apply** to commit the changes.

Clearing ARP Caches

You can clear the ARP cache from the ARP or IP Configuration window. In both windows, click the **Clear ARP Cache** button.

Configuring IP Source Routing

IP source routing allows you to configure the default route a packet should take based on the source IP address of the packet. This section provides information and procedures about configuring IP source routing on the Cuda 12000 and includes following:

- About IP Source Routing
- Adding a Source Route

About IP Source Routing

Source routing allows you to configure a different default route for each IP network or host. Specifically, source routing allows you to define the default route (next hop gateway*)* to which a packet containing a particular source IP address should be forwarded in the event that a local route to the destination does not exist. This feature is called source routing because the route is determined by the source of the message.

When an IP packet is received on an interface:

- The interface performs a normal destination-based route lookup.
- If the system finds no route, or if a default route exists for the destination IP address, it then checks the source routing entries defined on the interface.
- If the system finds a source routing entry defined for the source address, the packet is forwarded to the next hop gateway associated with the source address. Otherwise, the default route defined in the routing table is used.

This logic enables learned routes to take precedence over both default routes and source routing entries; but enables source routing entries to take precedence over default routes.

Source routing is configured on an interface on which you define these source routing criteria:

- **Source IP address to match**. An IP address and network mask combination that allows you to define the source route to match as a network, or scope it down to a specific host.

- **Next Hop Gateway**. The IP address to which the system must forward any matching IP datagrams. Note that you must enter a valid next hop destination.

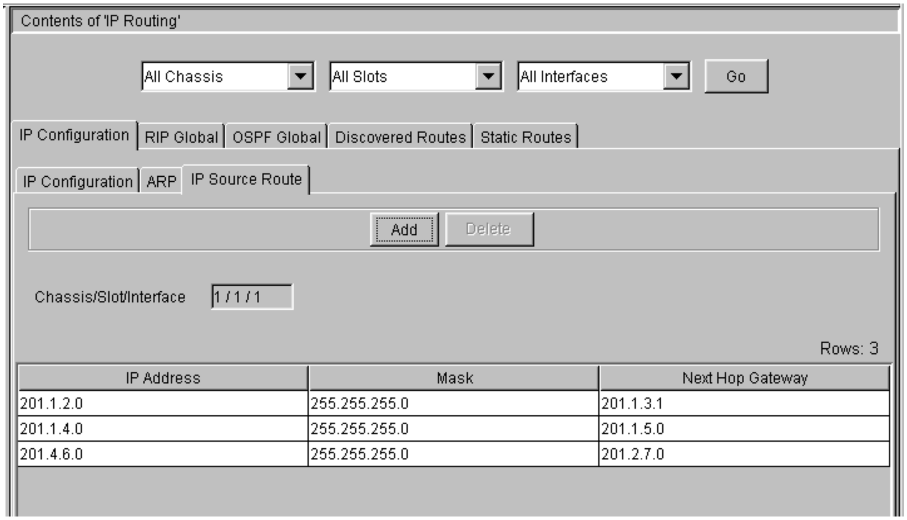
Adding a Source Route

Source routing is defined on a per-interface basis. To add a source route entry on a particular interface, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **IP** > **IP Routing**.
2. Click the **IP Configuration** tab.
3. Click the **IP Configuration** sub tab.
4. Select the row that includes the interface on which you want to add an IP source route.
5. Click the **IP Source Route** tab. The IP Source Route window opens and includes all source route entries configured on the interface.
6. Click **Add** to add an IP source route. The Add IP Source Route window opens as shown in the next figure.
7. Enter values for the parameters.
8. Click **OK** to commit the information or click **Cancel** to exit without saving.

What You See

Figure 12-8 IP Configuration IP Source Route Window



Chassis/Slot/Interface 1 / 1 / 1

Rows: 3

IP Address	Mask	Next Hop Gateway
201.1.2.0	255.255.255.0	201.1.3.1
201.1.4.0	255.255.255.0	201.1.5.0
201.4.6.0	255.255.255.0	201.2.7.0

Parameter Descriptions

This table provides a description of the IP Source Route window

Table 12-4 IP Source Route Window Parameters

Parameter	Description
IP Address	Source IP address for packets originating at that interface.
Mask	Network mask for that interface.
Next Hop Gateway	Next hop gateway for packets originating at the interface.

Configuring RIP Global

RIP (Routing Internet Protocol) is a broadcast-based protocol that routers use to periodically update routing tables, which include information about the networks that are in their routing tables. The routing table is broadcast to the other routers on the network where RIP is configured over IP.

Configuring RIP involves configuring RIP Interfaces, and Import and Export Filters. Refer to Chapter 9 for information on Importing and Exporting filters.

RIP Interfaces

The Cuda 12000 supports RIP version 2 as defined in RFC 2354. The Cuda 12000 can interoperate in a network of both RIPv1 and RIPv2 routers. A network composed of RIPv1 and RIPv2 routers is useful in supporting the transition from older routers to newer routers supporting RIPv2.

To exchange RIP routes over an interface you must configure RIP over IP on that interface. After you add RIP to the interface, the Cuda 12000 begins to exchange RIP routes with adjacent RIP routers.

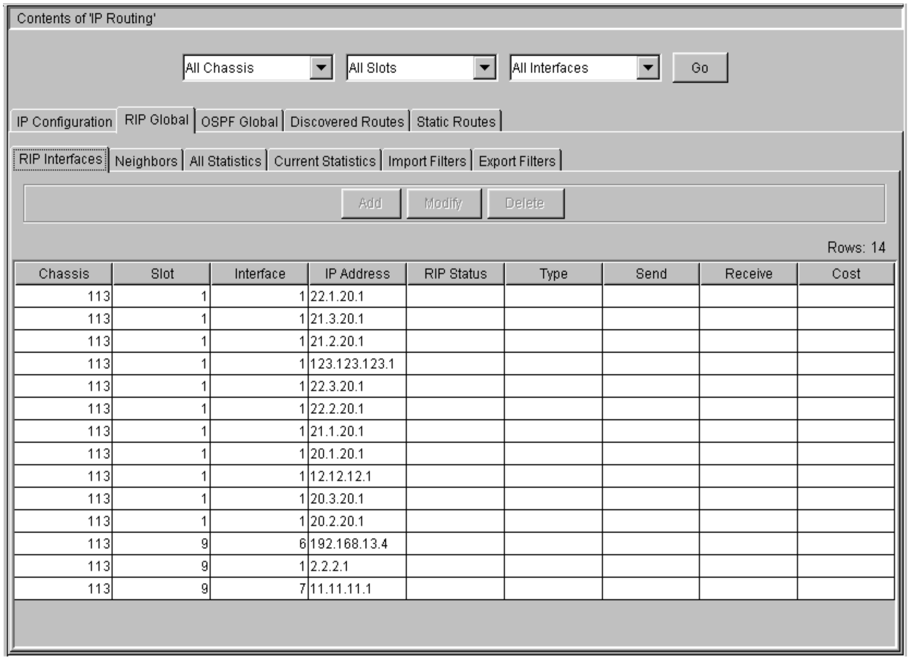
Before You Begin

Before you configure the RIP interfaces, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **IP** > **IP Routing**.
2. Click the **RIP Global** tab. The RIP Global window appears.
3. Click the **RIP Interfaces** tab. The RIP Interface window appears that includes an entry for each physical interface configured with an IP address.

What You See

Figure 12-9 RIP Interfaces Window



Rows: 14

Chassis	Slot	Interface	IP Address	RIP Status	Type	Send	Receive	Cost
113	1	1	22.1.20.1					
113	1	1	21.3.20.1					
113	1	1	21.2.20.1					
113	1	1	123.123.123.1					
113	1	1	22.3.20.1					
113	1	1	22.2.20.1					
113	1	1	21.1.20.1					
113	1	1	20.1.20.1					
113	1	1	12.12.12.1					
113	1	1	20.3.20.1					
113	1	1	20.2.20.1					
113	9	6	192.168.13.4					
113	9	1	2.2.2.1					
113	9	7	11.11.11.1					

Parameter Descriptions

This table provides a description of the **RIP Interface** window.

Table 12-5 RIP Interface Window Parameters.

Parameter	Description
Chassis	Indicates the chassis.
Slot	Indicates the slot.
Interface	Indicates the interface.
IP Address	The IP address of the Cuda 12000 IP interface.
RIP Status	Indicates which version of RIP packets this router will send on this interface. You may choose from RIPv1, RIPv2, RIPv1 Compatible, or none.
Type	Indicates the method of authenticating RIP packets on this interface.

Parameter	Description
Send	Indicates which version of RIP packets this router sends on this interface. The options are: RIPv1, RIPv2, RIPv1 compatible, or none.
RIPv2	Sends routes over a multicast IP address.
RIPv1	Compatible sends routes as RIPv2, however, over a broadcast IP address
Receive	Indicates which versions of RIP packets the router accepts on this interface. You may choose from RIPv1, RIPv2, both or none.
cost	Indicates the metric value that is to be added to the route metric of the routes advertised through this RIP interface.

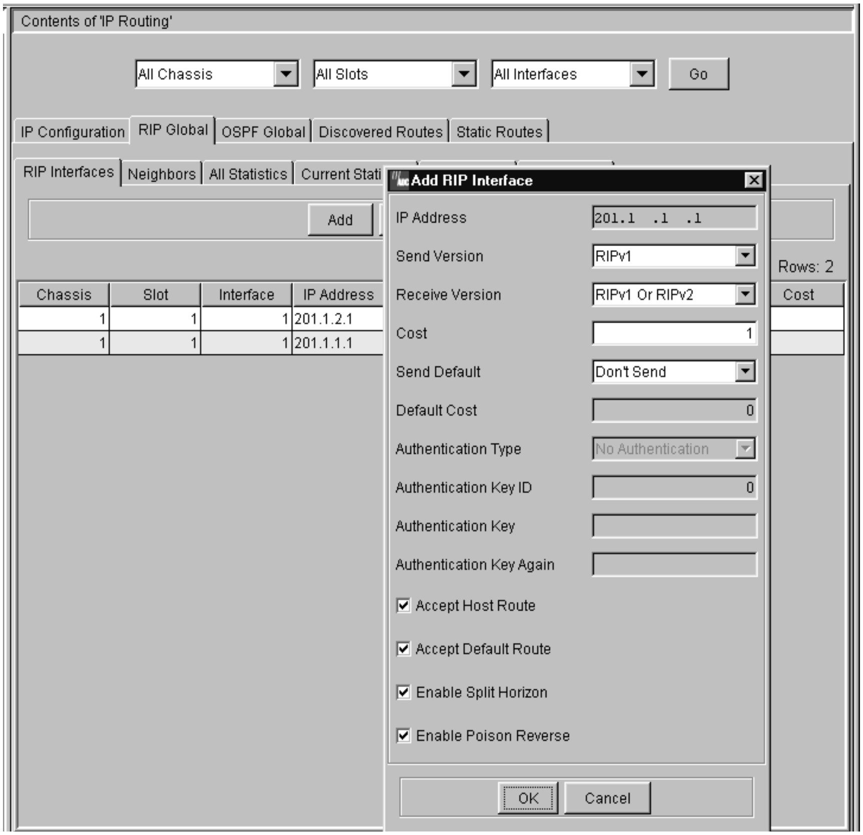
Adding a RIP Interface

Configuring a RIP interface involves adding RIP over an interface. After RIP is added to the interface the Cuda 12000 begins to exchange RIP routes with adjacent RIP routers. To configure RIP interface, follow this procedure:

1. In the RIP Global window, click the **RIP Interfaces** tab.
2. Select the row that includes the interface over which you wish to add a RIP interface.
3. Click **Add**. The Add RIP Interface window appears.
4. Enter values for the parameters. Refer to Table 12-6.
5. Click **OK** to commit the information or click **Cancel**.

What You See

Figure 12-10 Add RIP Interface Window



Contents of 'IP Routing'

All Chassis | All Slots | All Interfaces | Go

IP Configuration | RIP Global | OSPF Global | Discovered Routes | Static Routes

RIP Interfaces | Neighbors | All Statistics | Current Stati

Add

Rows: 2

Chassis	Slot	Interface	IP Address	Cost
1	1	1	201.1.2.1	
1	1	1	201.1.1.1	

Add RIP Interface

IP Address	201.1 .1 .1
Send Version	RIPv1
Receive Version	RIPv1 Or RIPv2
Cost	1
Send Default	Don't Send
Default Cost	0
Authentication Type	No Authentication
Authentication Key ID	0
Authentication Key	
Authentication Key Again	

☑ Accept Host Route

☑ Accept Default Route

☑ Enable Split Horizon

☑ Enable Poison Reverse

OK | Cancel

Parameter Descriptions

This table provides a description of the Add RIP Interface window.

Table 12-6 Add RIP Interface Parameter Descriptions

Parameter	Description
IP Address	Read only. IP address for this interface.

Parameter	Description
Send Version	What the router sends on this interface.Multiple Send versions. Version1 implies sending RIP updates compliant with RFC 1058. ripSendVer2 implies multicasting RIP-2 updates. *NOTE: You must indicate RIPv2 in order to authenticate.*
Receive Version	This indicates which version of RIP updates is to be accepted. Note that ripRcvVer2 and ripRcvVer1and2 implies reception of multicast packets
Cost	Value of metric corresponding to this interface. Metric value is added to all routes learned from this interface.
Send Default	If TRUE, RIP update from this interface include the default route.
Default Cost	This variable indicates the metric to be used for the default route entry in RIP updates originated on this interface.
Authentication Type	Type of authentication used on the interface. The options are no authentication, MD5 or simple password.
Authentication Key ID	The md5 authentication key id used for this interface. RFC2082 describes md5 authentication and key ids. A range of 1 to 255 is allowed.
Authentication Key	The value to be used as the Authentication Key whenever the corresponding instance of Authentication Type has a value other than no Authentication. A modification of the corresponding instance of Auth.Type does not modify the Auth. Key value. If a string shorter than 16 octets is supplied, it is left- justified and padded to 16 octets, on the right, with nulls (0x00). Reading this object always results in an OCTET string of length zero; authentication may not be bypassed by reading the MIB object.
Authentication Key Again	TRUE enables authentication on this interface. All updates generated from this interface are authenticated based on authentication type.
Accept Host Route	If FALSE, then host routes are NOT accepted on this interface
Accept Default Route	If TRUE, then default routes are accepted on this interface.
Enable Split Horizon	If TRUE, this enables split horizon processing as defined in RFC 2354.

Parameter	Description
Enable Poison Reverse	If TRUE, this enables Poison reverse updates on this interface.

Modifying RIP Interfaces

To modify a RIP Interface follow this procedure:

1. In the RIP Global window, click the **RIP Interfaces** tab.
2. Select the row that includes the interface that you wish to modify.
3. Click **Modify**. The Modify RIP Interface window appears.
4. Update parameters as necessary.
5. Click **OK** to commit the information or click **Cancel**.

Deleting RIP Interfaces

To delete a RIP Interface, follow this procedure:

1. From the RIP Global window, click the **RIP Interfaces** tab.
2. Select the row that includes the interface that you wish to delete.
3. Click **Delete**. A confirmation window appears.
4. Click **Yes** to continue or click **Cancel**.

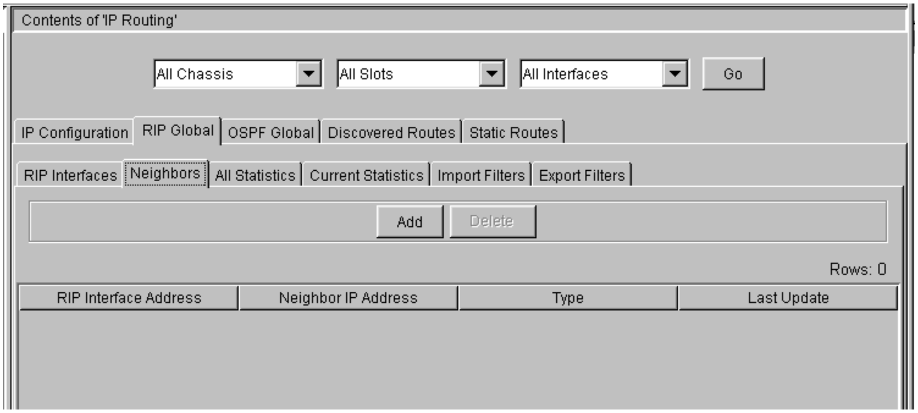
Viewing RIP Neighbors

To view RIP neighbors, follow this procedure:

1. In the RIP Global window, click the **Neighbors** tab.

What You See

Figure 12-11 Neighbors Window



RIP Interface Address	Neighbor IP Address	Type	Last Update

Parameter Descriptions

This table provides a description of the Neighbors window.

Table 12-7 Neighbors Window Parameter Descriptions

Parameter	Description
RIP Interface Address	IP address of the RIP interface to the neighbor.

Parameter	Description
Neighbor IP Address	IP address of the neighbor.
Type	A neighbor is of type Configured if it is configured on the interface. A neighbor is of type Discovered (discovered dynamically) if it is not configured, and updates from this neighbor are received on this interface.
Last Update	Time since last update was received from this neighbor. Read-only.

Adding a RIP Neighbor

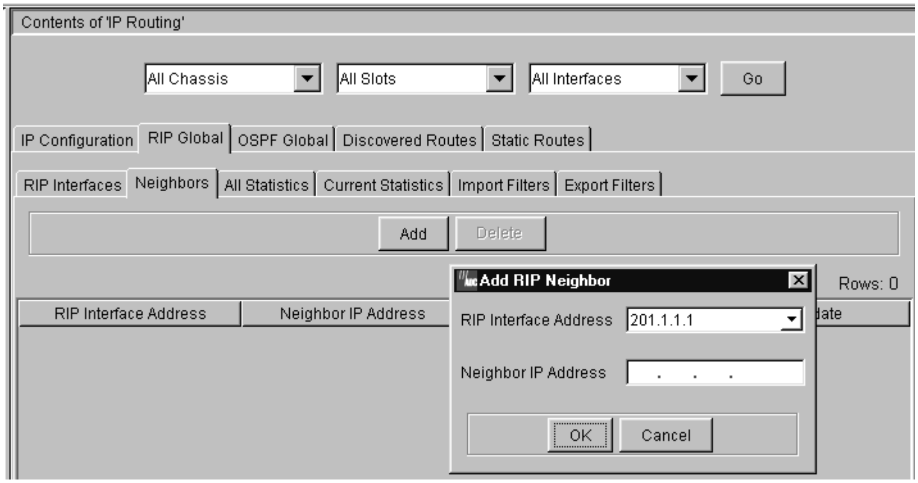
To add a RIP neighbor, follow this procedure:

1. In the RIP Global window, click the **Neighbors** tab.
2. Click **Add**. The Add RIP Neighbor window appears.
3. Enter values for the parameters. Refer to Table 12-8.
4. Click **Ok** to commit or click **Cancel** to exit without saving.

Note: You must have configured at least one RIP interface first.

What You See

Figure 12-12 Add RIP Neighbor Window



Contents of 'IP Routing'

Add RIP Neighbor

RIP Interface Address: 201.1.1.1

Neighbor IP Address: . . .

Rows: 0

Parameter Descriptions

This table provides a description of the Add RIP Neighbor window.

Table 12-8 Add RIP Neighbor Window Parameters

Parameter	Description
RIP Interface Address	IP address of the RIP interface to the neighbor.
Neighbor IP Address	IP address of the neighbor.

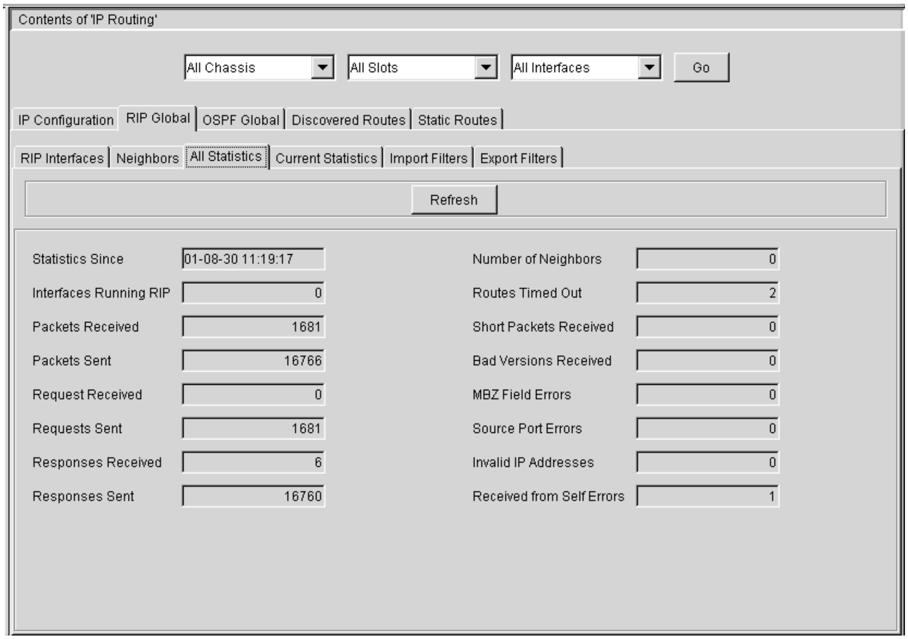
Viewing RIP Statistics

To view RIP statistics, follow this procedure:

1. In the RIP Global window, click the **All Statistics** tab.
2. Click **Refresh** to update the information

What You See

Figure 12-13 All Statistics Window



Statistics Since	01-08-30 11:19:17	Number of Neighbors	0
Interfaces Running RIP	0	Routes Timed Out	2
Packets Received	1681	Short Packets Received	0
Packets Sent	16766	Bad Versions Received	0
Request Received	0	MBZ Field Errors	0
Requests Sent	1681	Source Port Errors	0
Responses Received	6	Invalid IP Addresses	0
Responses Sent	16760	Received from Self Errors	1

Parameter Descriptions

This table provides a description of the All Statistics window.

Table 12-9 All Statistics Parameter Descriptions

Parameter	Description
Statistics Since	Time last stats cleared.
Interfaces Running RIP	Number of enabled interfaces running RIP.
Packets Received	Total number of RIP packets received on all interfaces.
Packets Sent	Total number of RIP packets sent out on all interfaces.
Request Received	Total number of RIP requests received on all interfaces.
Requests Sent	Total number of RIP requests sent out on all interfaces.
Responses Received	Total number of RIP responses received on all interfaces.
Responses Sent	Total number of RIP responses sent out on all interfaces.
Number of Neighbors	Total number of neighbors of all RIP interfaces.
Routes Timed Out	Total number of RIP routes timed out.
Short Packets Received	Total number of RIP packets with size less than RIP header size received on all interfaces.
Bad Versions Received	Total number of RIP packets with version other than RIP version 1 or RIP version 2, received on all interfaces.
MBZ Field Errors	Total number of RIP packets with must be zero fields not set to zero received on all interfaces.
Source Port Errors	Total number of RIP packets which did not originate from port 520, received on all interfaces.
Invalid IP Address	Total number of RIP packets with invalid ip address, received on all interfaces.
Received from Self Errors	Total number of RIP packets with receiver being the sender on all interfaces.

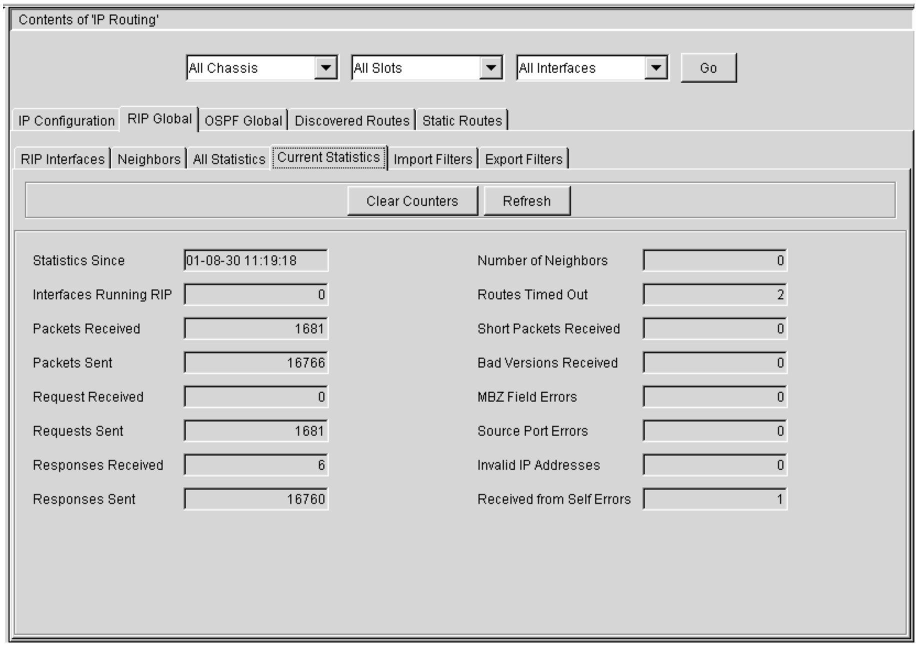
Viewing Current Statistics

To view the current statistics, follow this procedure:

1. In the RIP Global window, click the **Current Statistics** tab.
2. Click **Refresh** to update the information

What You See

Figure 12-14 Current Statistics Window



Statistics Since	01-08-30 11:19:18	Number of Neighbors	0
Interfaces Running RIP	0	Routes Timed Out	2
Packets Received	1681	Short Packets Received	0
Packets Sent	16766	Bad Versions Received	0
Request Received	0	MBZ Field Errors	0
Requests Sent	1681	Source Port Errors	0
Responses Received	6	Invalid IP Addresses	0
Responses Sent	16760	Received from Self Errors	1

Parameter Descriptions

This table provides a description of the Current Statistics window.

Table 12-10 Current Statistics Window Parameters

Parameter	Description
Statistics Since	Time last stats cleared.
Interfaces Running RIP	Number of enabled interfaces running RIP.

Parameter	Description
Packets Received	Total number of RIP packets received on all interfaces.
Packets Sent	Total number of RIP packets sent out on all interfaces.
Request Received	Total number of RIP requests received on all interfaces.
Requests Sent	Total number of RIP requests sent out on all interfaces.
Responses Received	Total number of RIP responses received on all interfaces.
Responses Sent	Total number of RIP responses sent out on all interfaces.
Number of Neighbors	Total number of neighbors of all RIP interfaces.
Routes Timed Out	Total number of RIP routes timed out.
Short Packets Received	Total number of RIP packets with size less than RIP header size received on all interfaces.
Bad Versions Received	Total number of RIP packets with version other than RIP version 1 or RIP version 2, received on all interfaces.
MBZ Field Errors	Total number of RIP packets with must be zero fields not set to zero received on all interfaces.
Source Port Errors	Total number of RIP packets which did not originate from port 520, received on all interfaces.
Invalid IP Address	Total number of RIP packets with invalid ip address, received on all interfaces.
Received from Self Errors	Total number of RIP packets with receiver being the sender on all interfaces.

Configuring OSPF Global

OSPF (Open Shortest Path First) is a link-state routing protocol. The Cuda 12000 supports OSPF version 2 as defined in RFC 1583. Configuring OSPF involves these functions.

- Configuring OSPF Global Parameters
- Viewing OSPF Areas
- Defining OSPF Areas
- Modifying OSPF Areas
- Deleting an OSPF Area Parameter
- Defining OSPF Area Ranges

All OSPF protocol exchanges are authenticated.This means that only trusted routers can participate in routing within an autonomous system.

Refer to Chapter 13, "Creating Route Filters" for an explanation of how to configure OSPF Import and Export Filters.

Before You Begin

Before you configure the RIP interfaces, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **IP** > **IP Routing**.
2. Click the **OSPF Global** tab. The OSPF Global window appears.

Configuring OSPF Global Parameters

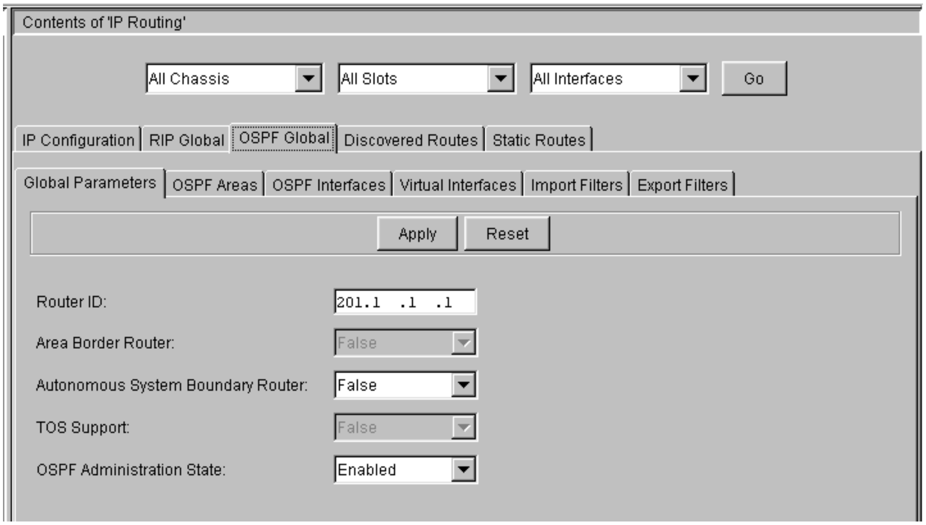
OSPF Global Parameters provide network information about OSPF. To configure the global parameters, follow this procedure:

1. In the OSPF Global window, click the **Global Parameters** tab. The **Global Parameters** window appears.
2. Enter values for the parameters. Refer to Table 12-11.
3. Click **Apply** to commit the information or click **Reset** to return to the previous values.

What You See

This figure shows an example of the Global Parameters window.

Figure 12-15 OSPF Global Parameters Window



Contents of 'IP Routing'

All Chassis | All Slots | All Interfaces | Go

Router ID: 201.1 .1 .1

Area Border Router: False

Autonomous System Boundary Router: False

TOS Support: False

OSPF Administration State: Enabled

Parameter Descriptions

This table provides a description of the Global Parameters window.

Table 12-11 OSPF Global Parameters Window Description

Parameter	Description
Router ID	Router ID to be used by OSPF. Be sure to change the default router ID to a unique router ID unique to your network
Area Border Router	Specifies if the router of the OSPF neighbor that acts as the Area Border Router between the transit area and the backbone. Values are True or False.
Autonomous System Border Router (ASBR)	Specifies if router is a border router sitting between OSPF areas.
TOS Support	Supports TOS. Values are True or False.
OSPF Administration State	Enables or Disables OSPF interface.

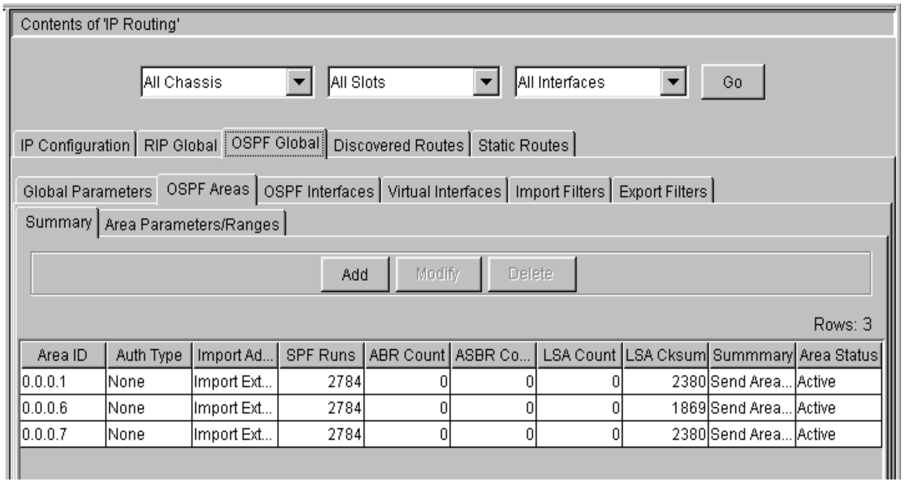
Viewing OSPF Areas

To view OSPF Area parameters follow these steps:

1. In the OSPF Global window, click the **OSPF Areas** tab. The OSPF Areas window appears.
2. Click the **Summary** tab. The Summary window appears.

What You See

Figure 12-16 OSPF Areas Summary Window



Area ID	Auth Type	Import Ad...	SPF Runs	ABR Count	ASBR Co...	LSA Count	LSA Cksum	Summmary	Area Status
0.0.0.1	None	Import Ext...	2784	0	0	0	2380	Send Area...	Active
0.0.0.6	None	Import Ext...	2784	0	0	0	1869	Send Area...	Active
0.0.0.7	None	Import Ext...	2784	0	0	0	2380	Send Area...	Active

Parameter Descriptions

This table provides a description of the **OSPF Areas** window

Table 12-12 OSPF Areas Window Parameter Descriptions.

Parameter	Description
Area ID	ID that identifies this area to other routers in the autonomous system.
Auth Type	Authentication type for this area. The types are: Password and MD5.
Import Advertisement	The options are:
	Import External. Configures the router to import routes contained in external link state advertisements.

Parameter	Description
	Import No External. Configures the router to ignore routes contained in external link state advertisements.
SPF Runs	The number of times that the intra-area route table has been calculated using this area's link-state database. This is typically done using Dijkstra's algorithm.
ABR Count	The total number of area border routers reach- able within this area. This is initially zero, and is calculated in each SPF Pass.
ASBR Count	The total number of Autonomous System border routers reachable within this area. This is initially zero, and is calculated in each SPF Pass
LSA Cksum	The 32-bit unsigned sum of the LS checksums for link-state advertisements, that are contained in this area's link-state database. This sum excludes external (LS type 5) link-state advertisements. The sum can be used to determine if there has been a change in a router's link state data- base, and to compare the link-state database of two routers.
Summary	Shows whether summary link state advertisements are to be sent.
Area Status	Shows whether this area is currently Active or Inactive.

Defining OSPF Areas

You can divide an autonomous system into smaller, more manageable sub-divisions called areas. This serves to reduce the size of each router’s routing database. It reduces the amount of routing information that must travel through the network.

The Cuda 12000 supports two OSPF Area parameters configuration functions:

- Defining stub areas
- Assigning specific costs to the default summary route.

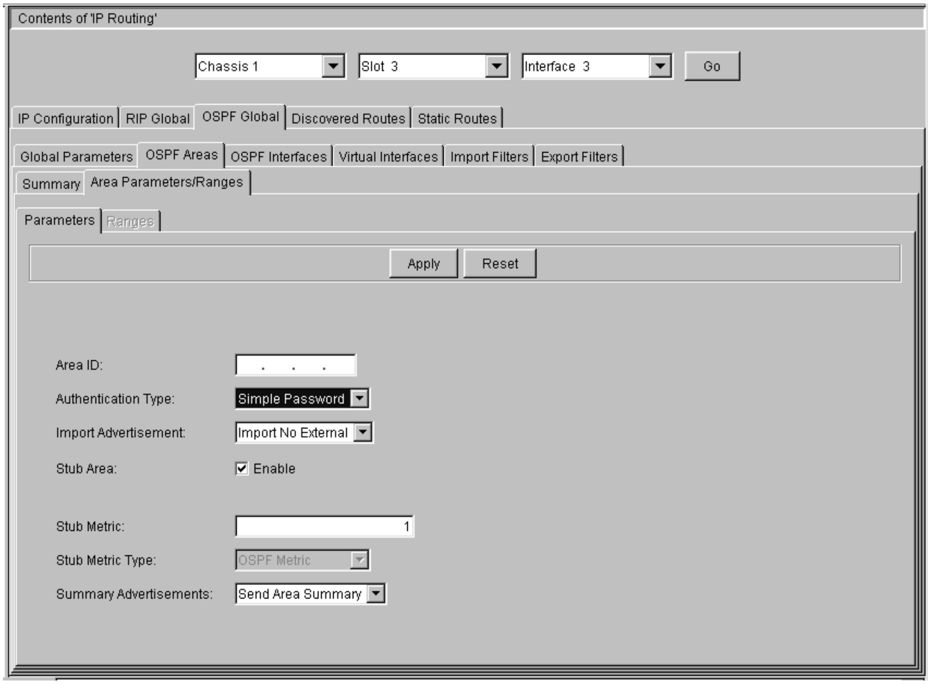
To define OSPF Area parameters, follow this procedure:

1. In the OSPF Global window, click the **OSPF Areas** tab.
2. Click the **Summary** tab. The Summary window appears.

3. Click **Add.** The Areas Parameters/Ranges window appears.
4. Enter values for the parameters. Refer to Table 12-13. You can enable the Stub Area parameter by setting the Import Advertisement to Import No External. If you enable the Stub Area parameter, several other parameters appear that you must configure. These additional parameters include:
   - Stub Metric
   - Stub-Metric Type
   - Summary Advertisements
5. Click **Apply** to save the configuration or click **Reset** to return to the previous values.

What You See

Figure 12-17 Areas Parameters window with the Stub Area Parameter Enabled.



Area ID: . . .

Authentication Type: Simple Password

Import Advertisement: Import No External

Stub Area: ☑ Enable

Stub Metric: 1

Stub Metric Type: OSPF Metric

Summary Advertisements: Send Area Summary

Parameter Descriptions

This table provides a description of the Areas Parameters window.

Table 12-13 OSPF Areas Parameters Window Description

Parameter	Description
Area ID	ID that identifies this area to other routers in the autonomous system. Enter 0.0.0.0 for a single area configuration or for a backbone area.
Authentication Type	Authentication type for this area (Password or MD5).
Import Advertisement	The options are:

Parameter	Description
Import External	Configures the router to import routes contained in external link state advertisements. If you select Import External as the advertisement method, your configuration is complete. Apply or Reset.
Import No External	Configures the router to ignore routes contained in external link state advertisements. Choose this selection if you want to define a stub area. If you have select Import No External as the import advertisement method, then enable the Stub Area parameter.
Stub Area	Stub areas do not accept or distribute external address advertisements. Instead, a single default external route injects into the area. Stub areas help minimize the routing table size of OSPF routers within the area. If you select Import No External as the import advertisement method, enable the Stub Area parameter. This expands the window and adds the Stub Metric, Stub Metric Type, and the Summary Advertisements parameters.
Stub Metric	Indicates the metric that is the default route entry in OSPF updates that are originated in this area. The range is from 1 to 16777215.
Stub Metric Type	Defines the type of metric advertised as a default route for the area. The options are:
OSPF Metric	An OSPF calculated metric.
Comparable Cost	External Type 1.
Non Comparable	External Type 2.
Summary Advertisements	The options are:
No Area Summary	The router neither originates nor propagates summary link-state advertisements (LSA) into the stub area. It relies entirely on its default route
Send Area Summary	The router both summarizes and propagates summary LSAs.

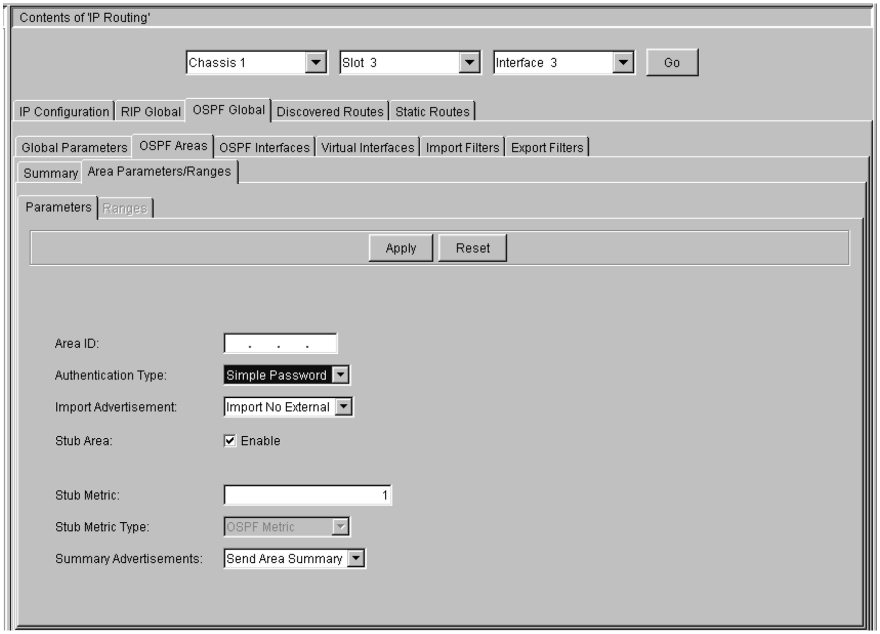
Modifying OSPF Area Parameters

To modify an OSPF Area Parameter, follow this procedure:

1. In the **OSPF Global** window, click the **OSPF Areas** tab.
2. Click the **Summary** tab.
3. Select the row that includes the Area ID that you wish to modify.
4. Click **Modify**. The Areas Parameters/Ranges window appears.
5. Update the values as necessary.
6. Click **Apply** to save the configuration or click **Reset** to the previous values.

What You See

Figure 12-18 Modify Areas Parameters Window



Contents of 'IP Routing'

Chassis 1 | Slot 3 | Interface 3 | Go

Area ID: . . .

Authentication Type: Simple Password

Import Advertisement: Import No External

Stub Area: ☑ Enable

Stub Metric: 1

Stub Metric Type: OSPF Metric

Summary Advertisements: Send Area Summary

Deleting an OSPF Area Parameter

Deleting an OSPF area consequently deletes all associated interface. To delete an OSPF Area Parameter, follow this procedure:

1. In the OSPF Global window, click the **OSPF Areas** tab.
2. Click the **Summary** tab.
3. Select the row that includes the Area ID that you wish to delete.
4. Click **Delete**. A confirmation window appears.
5. Click **Ok** to continue or click **Cancel**.

Defining OSPF Area Ranges

The purpose of creating area ranges is to perform route aggregation, which is the consolidation of advertised addresses. This feature causes a single summary route to be advertised to other areas by an area border router (ABR).

In OSPF, an ABR advertises networks in one area into another area. A group of more specific networks can be aggregated within a less specific network and advertised as such to reduce routing traffic.

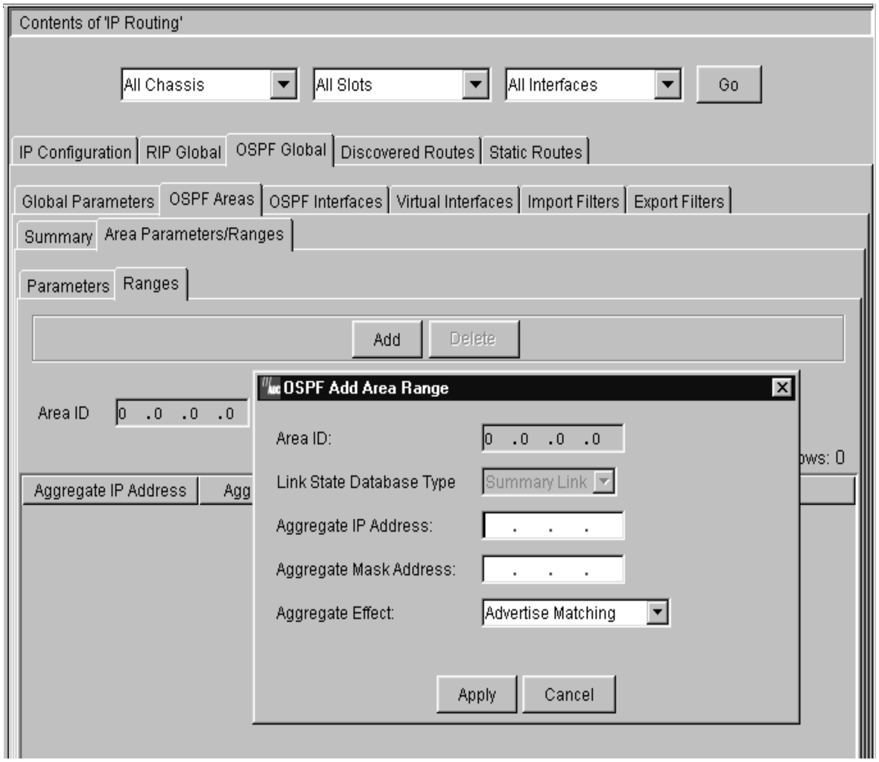
Ranges are defined after an OSPF Area Parameter is configured. Ranges are added to defined OSPF Area IDs.

To define an OSPF Area Range to an Area ID, follow this procedure:

1. In the OSPF Global window, click the **OSPF Areas** tab.
2. Click the **Summary** tab. The Summary window appears indicating the defined OSPF areas.
3. Select the row that includes the Area ID for the range you wish to define.
4. Click **Modify**. The Areas Parameters/Ranges window appears.
5. Click the **Ranges** tab. The Ranges window appears.
6. Click **Add**. The OSPF Add Area Ranges window appears. Refer to ().
7. Click **Apply** to save the configuration or click **Cancel** to exit without saving.

What You See

Figure 12-19 OSPF Add Area Range Window



Area ID: 0 .0 .0 .0

Link State Database Type: Summary Link

Aggregate IP Address: . . .

Aggregate Mask Address: . . .

Aggregate Effect: Advertise Matching

Parameter Descriptions

This table provides a description of the OSPF Add Area Ranges window.

Table 12-14 OSPF Add Area Ranges Window Parameters

Parameter	Description
Area ID	ID that identifies this area to other routers in the autonomous system. Enter 0.0.0.0 for a single area configuration or for a backbone area.
Link-State Database Type	Type of link state advertisement. Each link state type has a separate advertisement format.
Aggregate IP Address	Link-State ID used as the LS Type Specific field in the OSPF Link State Advertisement

Parameter	Description
Aggregate Mask Address	Subnet Mask that pertains to the Net or Subnet.
Aggregate Effect	The options are:
Advertise Matching	Indicate whether to advertise matching, i.e. subnets subsumed by ranges either trigger the advertisement.
No Advertise Matching	Indicate that the subnets are not to be advertised at all outside this area.

Configuring OSPF Interfaces

The purpose of configuring OSPF on an interface is to provide the Cuda 12000 with the ability to exchange OSPF routes over an IP interface.

Configuration involves these functions:

- Adding OSPF Parameters.
- Viewing OSPF Neighbors
- Modifying the OSPF Interface within the OSPF Area.
- Deleting an OSPF interface.

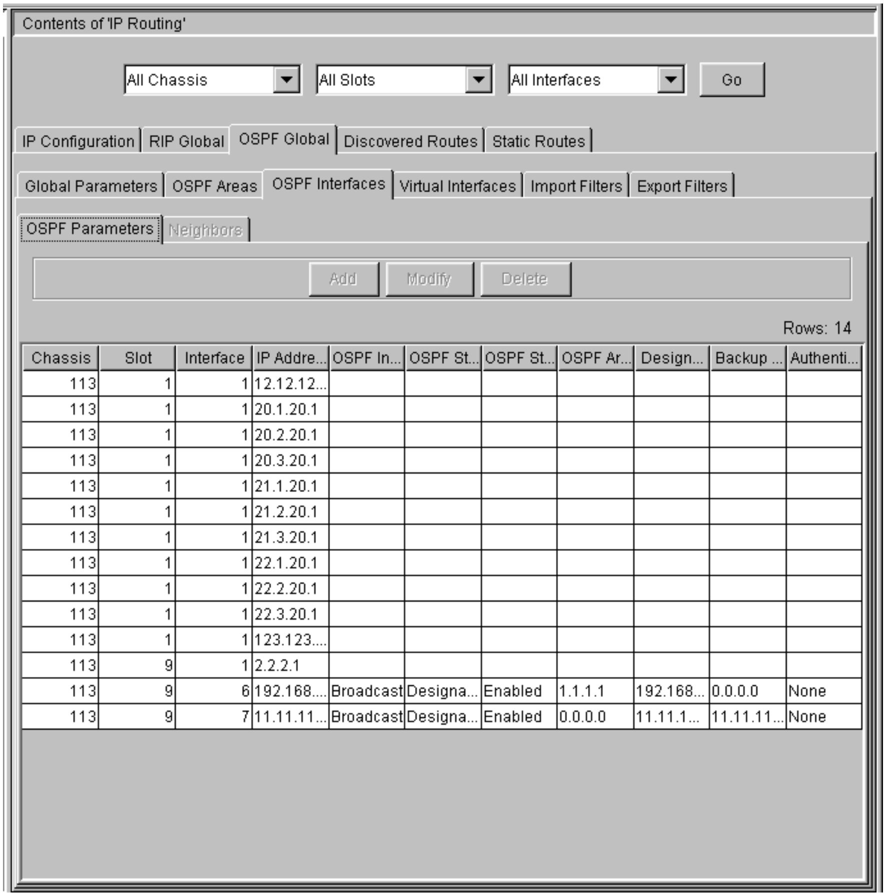
Before You Begin

Before you configure the OSPF interfaces, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **IP** > **IP Routing**.
2. Click the **OSPF Global** tab.
3. Click the **OSPF Interfaces** tab.
4. Click the **OSPF Parameters** tab. The OSPF Parameter window appears and provides a list of interfaces and IP Addresses, either configured or not configured with OSPF. Refer to the OSPF Interfaces Parameters table for more information.

What You See

Figure 12-20 OSPF Interfaces OSPF Parameters Window



Chassis	Slot	Interface	IP Addre...	OSPF In...	OSPF St...	OSPF St...	OSPF Ar...	Design...	Backup ...	Authenti...
113	1	1	12.12.12...							
113	1	1	20.1.20.1							
113	1	1	20.2.20.1							
113	1	1	20.3.20.1							
113	1	1	21.1.20.1							
113	1	1	21.2.20.1							
113	1	1	21.3.20.1							
113	1	1	22.1.20.1							
113	1	1	22.2.20.1							
113	1	1	22.3.20.1							
113	1	1	123.123....							
113	9	1	2.2.2.1							
113	9	6	192.168....	Broadcast	Designa...	Enabled	1.1.1.1	192.168...	0.0.0.0	None
113	9	7	11.11.11...	Broadcast	Designa...	Enabled	0.0.0.0	11.11.1...	11.11.11...	None

Parameter Descriptions

This table provides a description of the OSPF Interfaces OSPF Parameters window.

Table 12-15 OSPF Parameters Window Description

Parameter	Description
Chassis	Number you assign for the chassis in the network
Slot	Indicates the physical slot in which the cluster module is installed.

Parameter	**Description**
Interface	The module configured on the Cuda 12000.
IP Address	IP Address assigned to the Interface.
OSPF Interface Type	Corresponds to the physical Interface.
OSPF State	Displays state of OSPF. The states are Down and Designated Router.
OSPF Status	Indicates if OSPF is Enabled or Disabled for the Interface.
OSPF Area	Indicates the Area ID associated with OSPF for the Interface
Designated Rtr	Generates link state advertisement to routers in the same area and has several responsibilities for running the protocol. Elected by the Hello protocol. Its IP address is displayed.
Backup Rtr	The IP address of the backup designated router is displayed.
Authentication	This module defines a way Traceroute is used in the Cuda system.

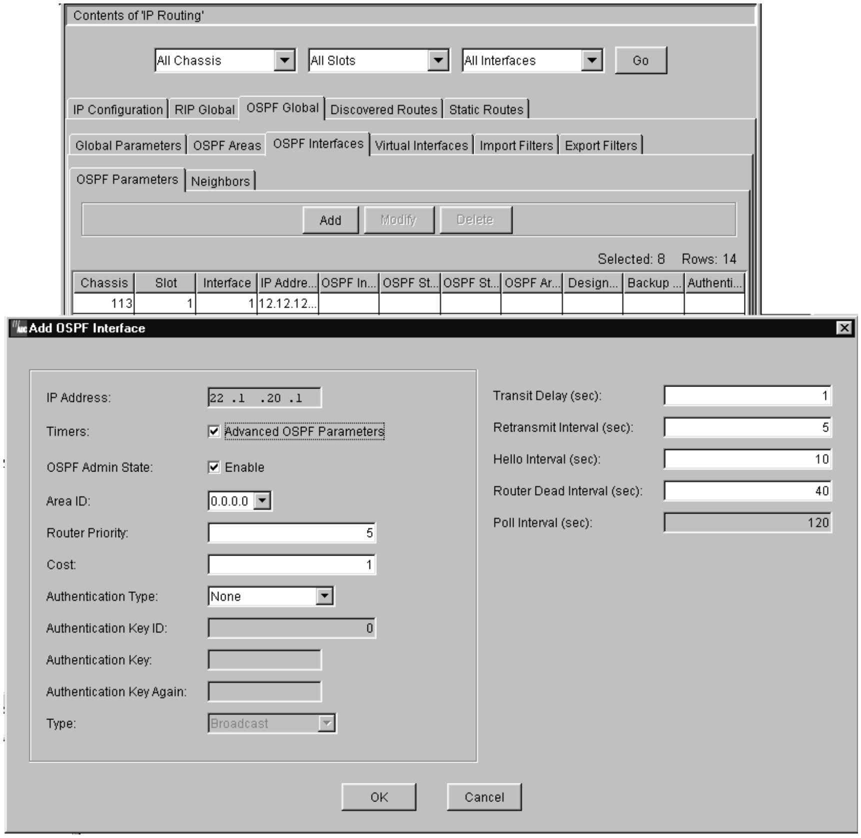
Adding OSPF Parameters

Follow these steps to configure OSPF Parameters on an IP Interface:

1. In the OSPF Parameters window, click **Add.** The Add OSPF Interface window appears.
2. Enter values for the parameters. Selecting the Timers parameters activates the parameters in the right column. Refer to Table 12-16.
3. Click **OK** to commit the information or click **Cancel** to exit without saving.

What You See

Figure 12-21 Add OSPF Interface Window



Selected: 8 Rows: 14

Chassis	Slot	Interface	IP Addre...	OSPF In...	OSPF St...	OSPF St...	OSPF Ar...	Design...	Backup ...	Authenti...
113	1	1	12.12.12...							

IP Address: 22 .1 .20 .1

Timers: ☑ Advanced OSPF Parameters

OSPF Admin State: ☑ Enable

Area ID: 0.0.0.0

Router Priority: 5

Cost: 1

Authentication Type: None

Authentication Key ID: 0

Authentication Key:

Authentication Key Again:

Type: Broadcast

Transit Delay (sec): 1

Retransmit Interval (sec): 5

Hello Interval (sec): 10

Router Dead Interval (sec): 40

Poll Interval (sec): 120

Parameter Descriptions

This table provides a description of the Add OSPF Interface window.

Table 12-16 Add OSPF Interface Window Parameters

Parameter	Description
IP Address	Read-only. The IP Interface selected to associate with an OSPF Area.
Timers	Enable to configure the following Advanced OSPF Parameters, to set timing specifications for the OSPF Interface.

Parameter	Description
Transit Delay (sec)	Estimated number of seconds it takes to transmit a link state update packet over this interface.
Retransmit Interval (sec)	Number of seconds between link-state advertisement retransmissions, for adjacencies belonging to this interface. This value is also used when retransmitting database description and link-state request packets.
Hello Interval (sec)	Length of time, in seconds, between the Hello packets that the Cuda 12000 sends on the interface. This value must be the same for all routers attached to a common network.
Router Dead Interval (sec)	Number of seconds that a router's Hello packets have not been seen before the Cuda 12000 declares the router down. This should be some multiple of the Hello interval. This value must be the same for all routers attached to a common network.
Poll Interval (sec)	Larger time interval, in seconds, between the Hello packets sent to an inactive non-broadcast multi-access neighbor.
OSPF Admin State	Specify whether to Enable or Disable the OSPF Interface.
Area ID	Select the Area in which to include this OSPF Interface.
Router Priority	Priority of the Cuda 12000 on this interface. Router Priority is used to elect a designated router on a multi-access network. In the event that another router is assigned the same priority, router election is a function of the Router ID. Acceptable values are 0-255. A value of zero signifies that the router is not eligible to become the designated router on this particular network
Cost	Metric for this interface. Acceptable values are 0-65535.
Authentication Type	Authentication type for an area.
Authentication Key	Authentication key for an area.
Type	Interface type that corresponds to the physical interface.

Viewing OSPF Neighbors

Neighbors are other OSPF routers on the same IP network. Each multi-access network that has at least two attached routers has a Designated Router. The Designated Router generates a link state advertisement for the multi-access network and has other special responsibilities in the running of the protocol. The Designated Router is elected by the Hello Protocol.

The Designated Router concept reduces the number of adjacencies required on a multi-access network. This, in turn, reduces the amount of routing protocol traffic and the size of the topological database.

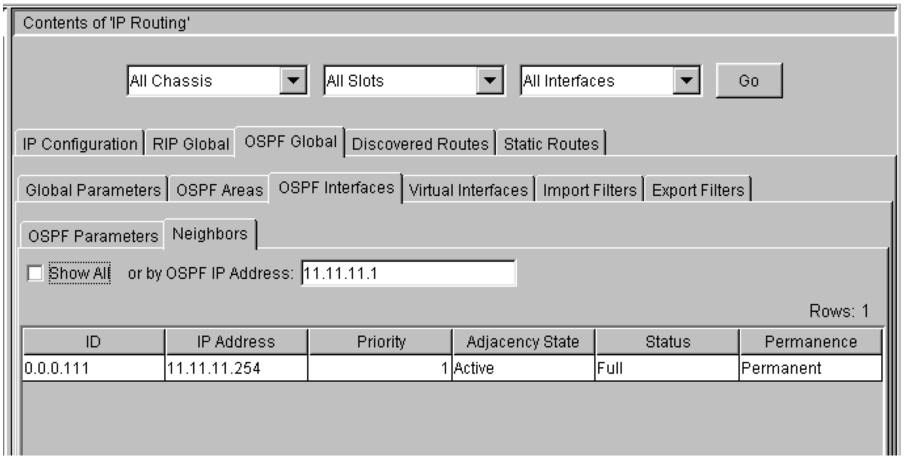
The Neighbors display allows you to view connectivity to other OSPF routers on the same network.

To view OSPF Neighbors, follow this procedure:

1. In the OSPF Parameters window, select the row that includes the OSPF IP Interface for the network that you wish to view.
2. Click the **Neighbors** tab. The Neighbors window appears and displays information for the neighbors on the same IP network as the OSPF configured IP address.

What You See

Figure 12-22 OSPF Neighbors Window



Contents of 'IP Routing'

All Chassis | All Slots | All Interfaces | Go

☐ Show All or by OSPF IP Address: 11.11.11.1

Rows: 1

ID	IP Address	Priority	Adjacency State	Status	Permanence
0.0.0.111	11.11.11.254	1	Active	Full	Permanent

Parameter Descriptions

This table provides a description of the OSPF Neighbors window.

Table 12-17 OSPF Neighbors Window Parameters

Parameter	Description
ID	ID of the OSPF neighbor.

Parameter	Description
IP Address	IP address of the neighboring router.
Priority	Priority of this neighbor in the designated router election algorithm. A value of zero signifies that the neighbor is not eligible to become the designated router on this particular network.
Adjacency State	State of the Neighbor from the perspective of the Cuda 12000. This is based upon the messages that the Cuda 12000 has received from the neighboring router. The options are: Down. Cuda 12000 has not heard from the neighbor within the period specified by the dead-interval OSPF interface configuration parameter. Attempt. This is a valid state only when OSPF is configured on a non-broadcast network. The attempt state indicates that no recent information has been received from the neighbor, but that a more concerted effort should be made to contact the neighbor. This is done by sending the neighbor Hello packets at intervals of Hello Interval. You can do this by configuring the Hello Interval on this interface. Init. The Cuda 12000 receives a OSPF Hello message from the neighboring router. However, bidirectional communication has not yet been established with the neighbor; that is the Cuda 12000 did not appear in the neighbor's Hello packet). All neighbors in this state (or higher) are listed in the Hello packets sent by the Cuda 12000 on the associated interface. Two Way. Communication between the Cuda 12000 and the neighboring router is now bidirectional. This has been assured by the fact that the Cuda 12000 is listed as a router in the last Hello packet received from the neighboring router. This is the most advanced state short of beginning adjacency establishment. The (Backup) Designated Router is selected from the set of neighbors in state 2-Way or greater. Exchange Start. This is the first step in creating an adjacency between the two neighboring routers. The goal of this step is to decide which router is the master, and to decide upon the initial DD sequence number. Neighbor conversations in this state or greater are called adjacencies. Exchange. In this state the Cuda 12000 is distributing its entire link state database by sending Database Description packets to the neighbor.

Parameter	Description
	Loading. In this state, Link-State Request packets are sent to the neighbor asking for the more recent advertisements that have been discovered (but not yet received) in the Exchange state. Full. The neighboring routers are fully adjacent. These adjacencies will now appear in router links and network links advertisements.
Status	A status of **Active** is displays for networks that contain more than one OSPF router.
Permanence	This variable displays the status of the entry. 'Dynamic' and 'permanent' refer to how the neighbor became known. Dynamic implies that the neighbor was learned. Permanent implies that the neighbor was configured (only for NBMA networks).

Configuring OSPF Virtual Interfaces

TOSPF requires that all areas be attached to the OSPF backbone area (area 0.0.0.0). However, you may encounter situations in which you cannot connect an OSPF area directly to the backbone. If your Cuda 12000 is an area border router between one area that is physically connected to the OSPF backbone and one area that is not, you can create a virtual interface on your Cuda 12000 to connect the non-contiguous area to the OSPF backbone.

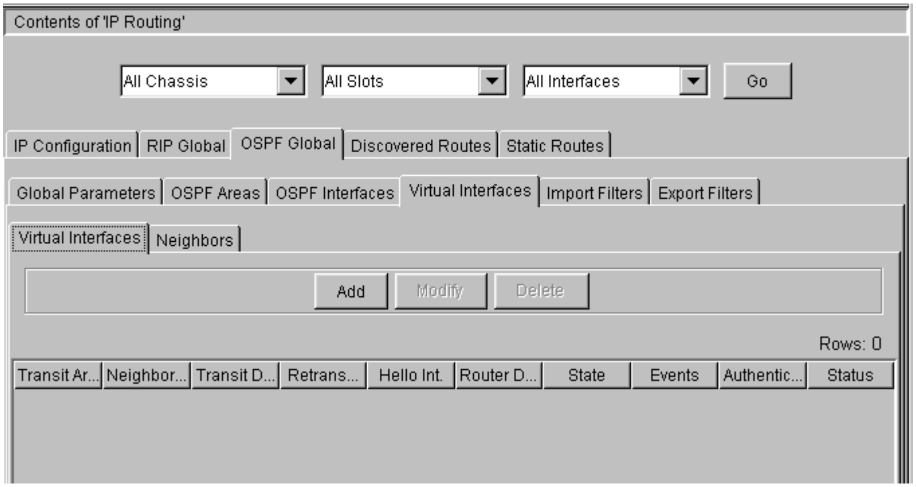
Before You Begin

Before you configure the OSPF virtual interfaces, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **IP** > **IP Routing**.
2. Click the **OSPF Global** tab.
3. Click the **Virtual Interfaces** tab.
4. Click the **Virtual Interfaces** sub tab.

What You See

Figure 12-23 OSPF Virtual Interfaces Window



Parameter Descriptions

This table provides a description of the OSPF Virtual Interfaces window.

Table 12-18 OSPF Virtual Interfaces Window Parameters]

Parameter	Description
Transit Area ID	The Transit Area that the Virtual Link traverses. By definition, this is not 0.0.0.0.
Neighbor Router ID	The Router ID of the Virtual Neighbor.
Transit Delay	The estimated number of seconds it takes to transmit a link-state update packet over this interface.
Retransmission	The number of seconds between link-state advertisement retransmissions, for adjacencies belonging to this interface. This value is also used when retransmitting database description and link-state request packets. This value should be well over the expected round- trip time.
Hello Interval	The length of time, in seconds, between the Hello packets that the router sends on the interface. This value must be the same for the virtual neighbor."
Router Dead	The number of seconds that a router's Hello packets have not been seen before it's neighbors declare the router down. This should be some multiple of the Hello interval. This value must be the same for the virtual neighbor.
State	OSPF virtual interface states. States are: Down, and Point-to-Point.
Events	The number of state changes or error events on this Virtual Link.
Authentication	If Authentication Type is simplePassword, the device will left adjust and zero fill to eight octets. Note that unauthenticated interfaces need no authentication key, and simple password authentication cannot use a key of more than eight octets.
Status	This variable displays the status of the entry. Setting it to 'invalid' has the effect of rendering it inoperative. The internal effect (row removal) is implementation- dependent.

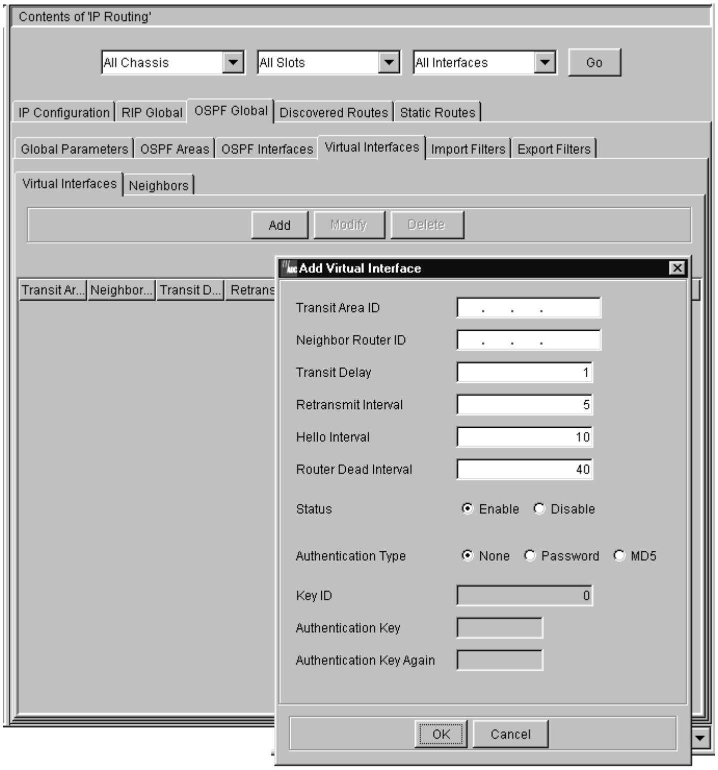
Adding a Virtual Interface

To add an OSPF interface, follow this procedure:

1. In the Virtual Interfaces window, click **Add.** The Add Virtual Interface window appears.
2. Enter values for the parameters. Refer to Table 12-19.
3. Click **OK** to commit the information or click **Cancel** to exit without saving.

What You See

Figure 12-24 Add OSPF Virtual Interface Window



Transit Area ID . . .
Neighbor Router ID . . .
Transit Delay 1
Retransmit Interval 5
Hello Interval 10
Router Dead Interval 40
Status ● Enable ○ Disable
Authentication Type ● None ○ Password ○ MD5
Key ID 0
Authentication Key
Authentication Key Again

Parameter Descriptions

This table provides a description of the Add OSPF Virtual Interface window.

Table 12-19 Add OSPF Virtual Interface Window Parameters

Parameter	Description
Transit Area ID	The Transit Area that the Virtual Link traverses. By definition, this is not 0.0.0.0.
Neighbor Router ID	The Router ID of the Virtual Neighbor.
Transit Delay	The estimated number of seconds it takes to transmit a link-state update packet over this interface.
Retransmit Interval	Number of seconds between link-state advertisement retransmissions, for adjacencies belonging to this interface. This value is also used when retransmitting database description and link-state request packets.
Hello Interval	Length of time, in seconds, between the Hello packets that the Cuda 12000 sends on the interface. This value must be the same for all routers attached to a common network.
Router Dead Interval	Number of seconds that a router's Hello packets have not been seen before the Cuda 12000 declares the router down. This should be some multiple of the Hello interval. This value must be the same for all routers attached to a common network.
Status	Enable/Disable.
Authentication Type	Authentication type for OSPF interface (None/Password/MD5).
Key ID	ID of MD5 authentication key (0 - 255).
Authentication Key	Octet string size(0 - 256). If the Area's Authentication Type is MD5, and the key length is shorter than 16 octets, the agent left-adjusts and zero fill to 16 octets.
Authentication Key	Repeat authentication key value.

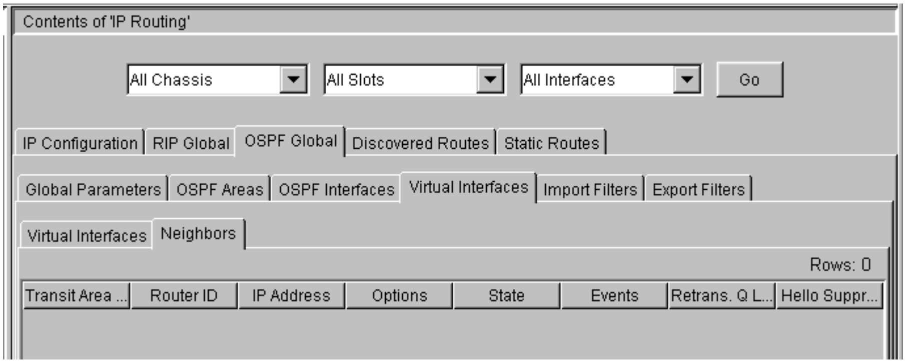
Viewing OSPF Neighbors

To view OSPF Neighbors, follow this procedure:

1. In the Virtual Interface window, select the row that includes the interface for the network that you wish to view.
2. Click the **Neighbors** tab. The Neighbors window appears and displays information for the neighbors on the same IP network as the OSPF configured IP address.

What You See

Figure 12-25 OSPF Neighbors Window



Parameter Descriptions

This table provides a description of the Neighbors window

Table 12-20 Virtual Interfaces Neighbors Window Parameters

Parameter	Description
Transit Area ID	The Transit Area that the Virtual Link traverses. By definition, this is not 0.0.0.0.
Neighbor Router ID	A 32-bit integer uniquely identifying the neighboring router in the Autonomous System.
IP Address	IP address used by the virtual neighbor.
Options	A Bit Mask corresponding to the neighbor's options field. Bit 1, if set, indicates that the system will operate on Type of Service metrics other than TOS 0. If zero, the neighbor will ignore all metrics except the TOS 0 metric. Bit 2, if set, indicates that the system is Network Multicast capable; that is, it implements OSPF Multicast Routing.
State	The state of the Virtual Neighbor Relationship: Values are :down (1), attempt (2), init (3), twoWay (4), exchangeStart (5), exchange (6), loading (7), full (8).
Event	The number of times this virtual link has changed its state, or an error has occurred.
Retransmit Q. Len.	The current length of the retransmission queue.
Hello Suppression	Indicates whether Hellos are being suppressed to the neighbor.

Viewing Discovered Routes

Cuda 12000 maintains a central routing table (RFC 2096 CIDR) that contains an entry for every *Discovered Route,* a learned or locally defined route. The routing table may contain up to 30,000 routes.

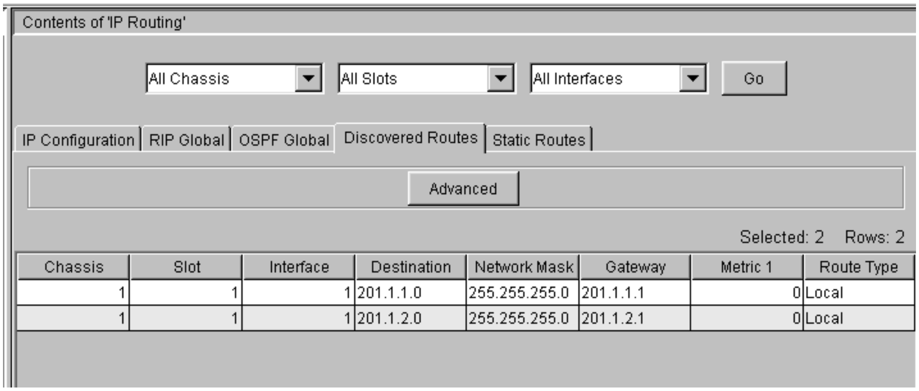
Before You Begin

Before you begin, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **IP** > **IP Routing**.
2. Click the **Discovered Routes** tab. The Discovered Routes window appears.

What You See

Figure 12-26 IP Routing Discovered Routes Window



Chassis	Slot	Interface	Destination	Network Mask	Gateway	Metric 1	Route Type
1	1	1	201.1.1.0	255.255.255.0	201.1.1.1	0	Local
1	1	1	201.1.2.0	255.255.255.0	201.1.2.1	0	Local

Parameter Descriptions

This table provides a description of the Discovered Routes window

Table 12-21 Discovered Routes Window Parameters.

Parameter	Description
Chassis	Number that you assign to the chassis in the network.
Slot	Indicates the physical slot in which the module resides.
Interface	Interface on which the route was discovered.
Destination	IP address of the destination network.

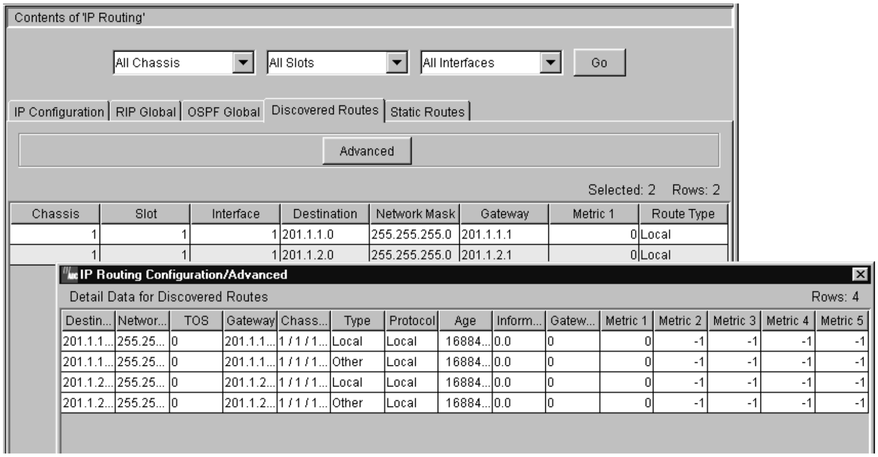
Parameter	Description
Network Mask	Subnet mask for the destination network.
Metric 1	Measure of distance to the destination. For RIP routes, this is the next hop. For OSPF routes, this is the cost.
Route Type	Indicates how the route was learned and put into the routing table.

Viewing Advanced Route Information

You may also display advanced routing information for each route entry. To view the advanced information, follow this procedure:

1. In the **Discovered Routes** window, click the Advanced tab.
2. Click **Refresh** to update the information.

Figure 12-27 Discovered Routes Advanced Routing Window



Selected: 2 Rows: 2

Chassis	Slot	Interface	Destination	Network Mask	Gateway	Metric 1	Route Type
1	1	1	201.1.1.0	255.255.255.0	201.1.1.1	0	Local
1	1	1	201.1.2.0	255.255.255.0	201.1.2.1	0	Local

IP Routing Configuration/Advanced

Detail Data for Discovered Routes Rows: 4

Destin...	Networ...	TOS	Gateway	Chass...	Type	Protocol	Age	Inform...	Gatew...	Metric 1	Metric 2	Metric 3	Metric 4	Metric 5
201.1.1...	255.25...	0	201.1.1...	1 / 1 / 1...	Local	Local	16884...	0.0	0	0	-1	-1	-1	-1
201.1.1...	255.25...	0	201.1.1...	1 / 1 / 1...	Other	Local	16884...	0.0	0	0	-1	-1	-1	-1
201.1.2...	255.25...	0	201.1.2...	1 / 1 / 1...	Local	Local	16884...	0.0	0	0	-1	-1	-1	-1
201.1.2...	255.25...	0	201.1.2...	1 / 1 / 1...	Other	Local	16884...	0.0	0	0	-1	-1	-1	-1

Parameter Descriptions

This table provides a description of the Discovered Routes Advanced Routing window

Table 12-22 Discovered Routes Advanced Routing Window Parameters.

Parameter	Description
Destination	IP address of the destination network.

Parameter	Description
Network Mask	Subnet mask for the destination network.
TOS	Type of service requested for this route. The type of service refers to a local policy for packets being forwarded by the Cuda 12000. A TOS of zero indicates that no local policy is used.
Gateway	IP address of the router interface through which the packet must travel to reach its next hop.
Chassis	Number you assign to the chassis in the network.
Type	Indicates how the route was learned and put into the routing table: Local, Remote, Reject, Other
Protocol	Protocol which installed the route in the routing database:
Age	Number of seconds since this route was last updated or otherwise determined to be correct.
Information	A reference to MIB definitions specific to the particular routing protocol which is responsible for this route, as determined by the value specified in the route's protocol field. If this information is not present, the information field is set to the 0,0.
Gateway AS	Autonomous System Number of the Next Hop. The semantics of this object are determined by the routing-protocol specified in the route's protocol field. When this object is unknown or not relevant its value is set to zero.
Metric 1	Primary routing metric for this route. The semantics of this metric are determined by the routing protocol specified in the route's Protocol field. If the Metric is not used, then its value is set to “-1.”
Metric 2 – Metric 5	Alternative routing matrices for this route. The semantics of this metric are determined by the routing protocol specified in the route's Protocol field. If the Metric is not used, then its value is set to “-1.”

Configuring Static Routes

You can manually add routes in the Cuda 12000 routing table. These routes are called ***static*** because they do not change in response to network topology changes and remain in the table until you manually remove them. They assist the dynamic routes in managing the exchange of data between routers.

Static routes are useful in network environments in which:

- No routing protocol is used, or
- You want to override select routes discovered using a routing protocol.

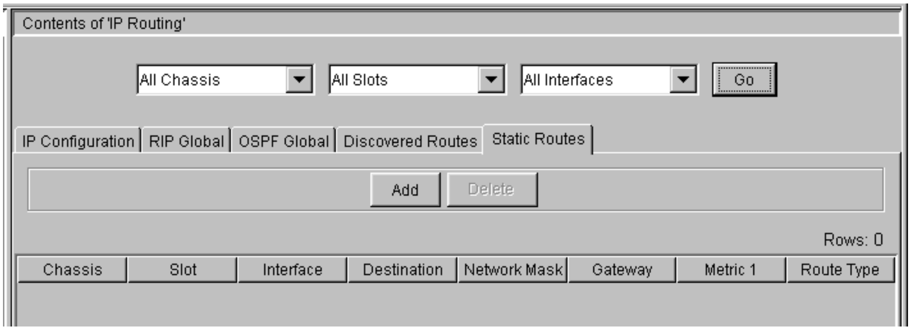
Before You Begin

Before you begin, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **IP** > **IP Routing.**
2. Click the **Static Routes** tab. The Static Routes window appears.

What You See

Figure 12-28 Static Routes Window



Chassis	Slot	Interface	Destination	Network Mask	Gateway	Metric 1	Route Type

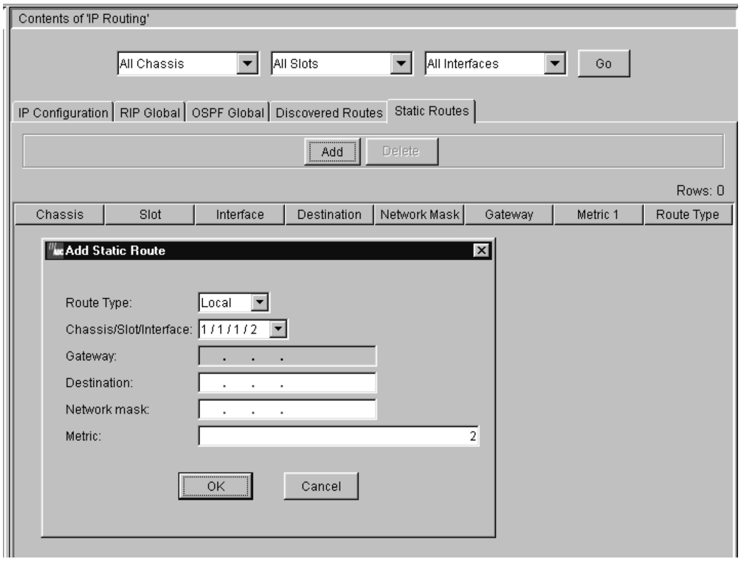
Adding a Static Route

To add a Static Route, follow this procedure:

1. In the Static Route window, click **Add.** The Add Static Route window appears.
2. Enter values for the parameters. Refer to Table 12-23.
3. Click **Ok** to commit the information or click **Cancel** to exit without adding the route.

What You See

Figure 12-29 Add Static Route Window



Rows: 0

Chassis	Slot	Interface	Destination	Network Mask	Gateway	Metric 1	Route Type

Route Type: Local

Chassis/Slot/Interface: 1 / 1 / 1 / 2

Gateway: . . .

Destination: . . .

Network mask: . . .

Metric: 2

Parameter Descriptions

This table provides a description of the Add Static Route window

Table 12-23 Add Static Route Window Parameters.

Parameter	Description
Route Type	The options are:

Parameter	Description
	Reject. This directs the Cuda 12000 to discard any packets destined to the specified destination network. Local. Configure a static route to a local destination via a specified interface. Remote. Configure a static route to a remote destination via a specified IP gateway. Default. Configure the default route for this router.
Chassis/Slot/Inte rface	Chassis/slot/interface that to which you are adding a static route.
Gateway	The next hop IP address. This is configured for only *Remote* routes.
Destination	IP address of the Destination network.
Network Mask	Network Mask assigned to this static route.
Metric	Assign a metric to this static route.

Deleting a Static Route

To delete a static route from the routing table, follow this procedure:

1. In the Static Route window, click **Delete.** A confirmation window appears.
2. Click **Yes** to continue or click **Cancel**.

13 CREATING ROUTE FILTERS

This chapter provides information and procedures on how to configure RIP and OSPF Route Filters.

Import and Export Route Filtering for RIP and OSPF

The Cuda 12000 uses route filtering functions to control the flow of routes to and from other RIP and OSPF routers. Two filtering functions are supported for control of RIP and OSPF routes; they are: *import* and *export*.

- Import — Controls how routes are added to the Cuda 12000 routing table.
- Export — Controls which routes are advertised to other routers.

In addition, route filtering customizes connectivity, increase security, conserve routing table space, or adjust route cost.

To understand route filtering, you must be familiar with these functions:

- Access Control Element (ACE) — A structure that defines the match criteria and the action that you want the Cuda 12000 to take for all routes that match the specified criteria.
- Access Control List (ACL) — A sequential grouping of ACEs. An incoming or outgoing route is compared against all ACEs that comprise the ACL. Whenever a route match is found, the system takes the action that is defined in the ACE.

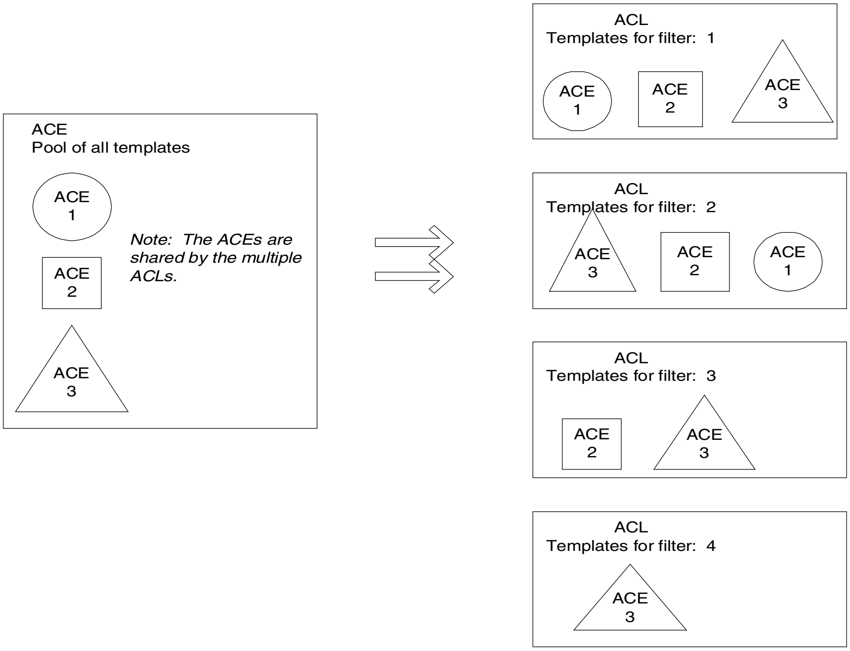
Defining RIP and OSPF route filtering is a two-step process:

- First, you create the ACEs to define both the match criteria and the action to take when a route match is found.
- Second, you create the ACL by selecting ACEs from a pool, and making them part of an ACL.

Following is an example that includes ACE templates 1, 2, and 3, and the ACLs created with these ACEs. Note the following from the example:

  - ACLs are made up of one or more ACEs.
  - The same ACE may be shared in multiple ACLs.
  - ACEs within each ACL must be sorted in order of the specific-to-general match criteria and action needs of the ACL.

Figure 13-1 Example of ACEs used to create ACLs



ACEs

An Access Control Element (ACE) is a structure used as a specification to match an incoming or outgoing route. ACEs contain the filtering criteria, as a template, and are used in Access Control Lists (ACLs) to determine the corresponding action to be taken when a routing match is successful.

Import ACEs dictate which routes are added to the Cuda's routing table.

Configuration involves creating an ACE by defining the specifications for the match criteria and action of a route.

⚠ Due to the membership relationship between ACEs and ACLs, it is recommended that ACE configuration and management be performed by an expert-level administrator.

Import and Export ACEs are automatically numbered sequentially when they are configured.

ACLs

An Access Control List (ACL) is a sequential grouping of ACEs that contain the filtering criteria. An incoming or outgoing route is compared against all ACEs that are added as ACLs. Whenever a route match is found, the system takes the action that is defined in the ACE.

Import filters dictate which routes are added to the Cuda's routing tables.

Configuration involves the following functions:

- Adding an ACL and selecting an ACE to be used by the ACL.
- Maneuvering ACEs to and from the ACL templates for filters.
- Choosing which ACL is to be the **Active** ACL. ACLs *must be activated* in order for the Cuda 12000 to recognize it.

Note: The configuration procedures and parameters contained within RIP and OSPF Import ACLs are the same.

Due to the membership relationship between ACEs and ACLs, it is recommended that ACL configuration and management be performed by an expert-level administrator.

Configuring Import ACEs

An Access Control Element (ACE) is a structure used as a specification to match an incoming or outgoing route.

Before You Begin

Before you begin to create route filters, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **IP** > **IP Routing.**
2. You can configure RIP route filters or OSPF route filters:
   - **a** To configure the RIP route filters, click the **RIP Global** tab.
   - **b** To configure the OSPF route filters, click the **OSPF Global** tab.
3. Click the **Import Filters** tab.

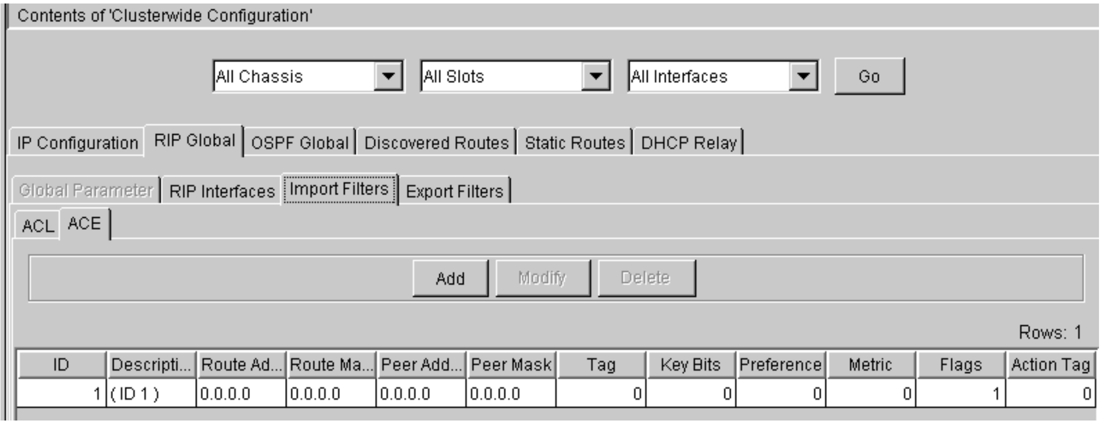
Creating RIP Import ACEs

This section describes how to create and add RIP Import ACEs that may be used to create ACLs. To create RIP Import ACEs follow this procedure:

1. In the **Import Filters** window, click the **ACE** tab. The ACE window appears and provides the existing ACEs that are available to be used for creating ACLs.
2. Click **Add**. The Adding RIP Import Template window appears.
3. Add values for the parameters.
4. Click **OK** to commit the information or click **Cancel** to exit without saving.

What You See

Figure 13-2 RIP Import Filters ACE Window



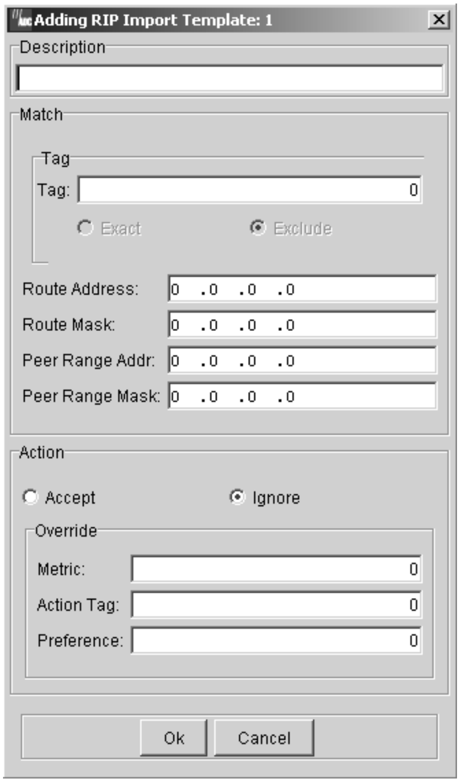
Contents of 'Clusterwide Configuration'

All Chassis | All Slots | All Interfaces | Go

Rows: 1

ID	Descripti...	Route Ad...	Route Ma...	Peer Add...	Peer Mask	Tag	Key Bits	Preference	Metric	Flags	Action Tag
1	(ID 1)	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0	0	0	0	1	0

Figure 13-3 Adding RIP Import Templates Window



Adding RIP Import Template: 1

Description

Match

Tag

Tag: 0

○ Exact ● Exclude

Route Address: 0 .0 .0 .0

Route Mask: 0 .0 .0 .0

Peer Range Addr: 0 .0 .0 .0

Peer Range Mask: 0 .0 .0 .0

Action

○ Accept ● Ignore

Override

Metric: 0

Action Tag: 0

Preference: 0

Parameter Descriptions

This table provides a description of the Adding RIP Import Template window parameters.

Parameter	Description
Description	Textual description to identify the ACE. The range is 0 to 64 alpha-numeric characters.
Match	Enter values for the match criteria. Any field left blank or set to zero is treated as “don’t care”.

Parameter	Description
Tag	Route tag to match against the value placed in the route tag field of the RIP packet by the sending router. *A Tag value cannot equal "0"*. The criteria options are: Exact — If the Tag field is specified, then enabling Exact indicates that the match is intended to match all routes with an exact match on the tag field. Exclude — If the Tag field is specified, then enabling Exclude indicates that the match is intended to match all routes that do not match on the tag field.
Route Address	Route address to match against incoming routes
Route Mask	Network mask to match against incoming routes.
Peer Range Addr	Peer IP address to match against incoming packets.
Peer Range Mask	Network mask for the peer IP address sending incoming packets. You can match on a single peer IP address or match on all peers from a range. For example, to match on a single peer enter the peer's IP address, and enter the network mask of 255.255.255.255. To match on all peers from a range enter the network address of 10.10.0.0 and enter the network mask of 255.255.0.0.
Action	Action criteria that you want the system to take when matching incoming RIP routes are found: Accept — Enable to accept the route information. Ignore — Enable to *ignore* the route information.
Metric	If a match is found and the Import action is Enabled, then substitute this metric for the metric specified for the incoming route. Acceptable values are 0-16.
Action Tag	If a match is found and the Import action is Enabled, then substitute this tag for the tag specified for the incoming route. Acceptable values are listed in the tooltip.
Preference	If a match is found and the Import action is Enabled, then use this preference when this route is added to the routing database. Acceptable values are 0-255.

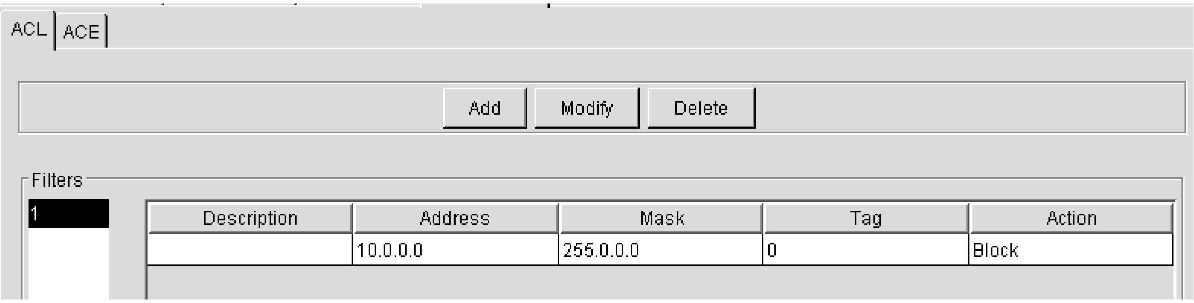
Modifying RIP Import ACEs

Modifying a RIP Import ACE involves removing the ACE as an ACL within the ACL configuration window, and changing the match criteria.

1. In the Import Filters window, click the **ACL** tab. The ACL window appears and provides the ACE for each ACL.
2. Select the row that includes the ACE you wish to modify. Click **Modify** [See Add RIP Imports Templates Window].
3. From the Templates for filter section, select the ACE and using the arrows, move it back to the Pools of all templates section.
4. Click **Ok** to commit or click **Cancel** to exit.
5. Click the **ACE** tab.
6. Select the row that includes the ACE that you wish to modify. Click **Modify**.
7. Modify parameters as necessary.
8. Click **Ok** to commit or click **Cancel** to exit.

What You See

Figure 13-4 RIP/OSPF Import Filters ACL Window



Description	Address	Mask	Tag	Action
	10.0.0.0	255.0.0.0	0	Block

Deleting RIP Import ACEs

Deleting a RIP Import ACE involves removing the ACE from an ACL within the ACL configuration window, and deleting it as an ACE within the ACE configuration window.

Before you delete an ACE, you must first remove it from each ACL of which that ACE is a member.

To delete an ACE follow this procedure:

1. In the Import Filters window, click the **ACL** tab. The ACL window appears and provides the ACE for each ACL.
2. From the Filter column, select the ACL you wish to delete or select the row that includes the ACE associated with the ACL you wish to delete.
3. Click **Modify**.
4. From the Templates for filter section, select the ACE and using the arrows, move it back to the Pools of all templates section.
5. Click **Ok** to commit or click **Cancel** to exit.
6. Click the **ACE** tab.
7. Select the row that includes the ACE that you wish to delete. Click **Delete**. A confirmation window appears.
8. Click **Yes** to continue or click **Cancel** to exit.

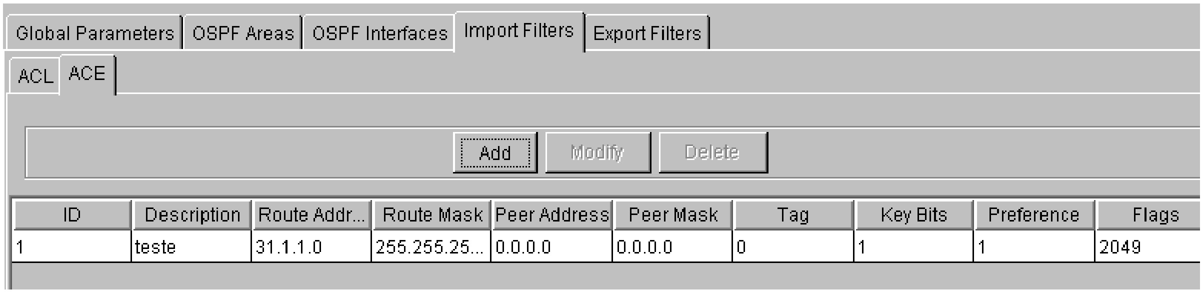
Creating OSPF Import ACEs

This section describes how to create and add OSPF Import ACEs that may be used to create OSPF ACLs. To create OSPF Import ACEs follow this procedure:

1. In the Import Filters window, click the **ACE** tab. The ACE window displays the ACEs that are available to be used for creating OSPF Import ACLs.
2. Click **Add**. The Adding OSPF Import Template window appears.
3. Enter values for the parameters.
4. Click **Ok** to commit or click **Cancel** to exit.

What You See

Figure 13-5 Add OSPF Import ACE window.



ID	Description	Route Addr...	Route Mask	Peer Address	Peer Mask	Tag	Key Bits	Preference	Flags
1	teste	31.1.1.0	255.255.25...	0.0.0.0	0.0.0.0	0	1	1	2049

Parameter Descriptions

This table provides a description of the Adding OSPF Import Template window parameters.

Parameter	Description
Description	Textual description to identify the ACE. The range is 0 to 64 alpha-numeric characters.
Match	Enter values for the match criteria. Any field left blank or set to zero is treated as "don't care".
Tag	Route tag to match against the value placed in the route tag field of the OSPF packet by the sending router. Choose one of these two criteria to tag a route: Exact — If the Tag field is specified, then enabling Exact indicates that the match is intended to match all routes with an exact match on the tag field. Exclude — If the Tag field is specified, then enabling Exclude indicates that the match is intended to match all routes that do not match on the tag field.
Route Address	Route Address key of the template.
Route Mask	Route Mask key of the template.
Peer Range Addr	Peer IP address to match against incoming packets.

Parameter	Description
Peer Range Mask	Network mask for the peer IP address sending incoming packets. You can match on a single peer IP address or match on all peers from a range. For example, to match on a single peer enter the peer's IP address, and enter the network mask of 255.255.255.255 To match on all peers from a range enter 1.1.0.0, and enter the network mask of 255.255.0.0.
Preference	If a match is found and the Import action is Enabled, then use this preference when this route is added to the routing database. Acceptable values are 0-255.

Modifying OSPF Import ACEs

Modifying an OSPF Import ACE involves removing the ACE from an ACL within the ACL configuration window, and deleting it as an ACE within the ACE configuration window. To modify an OSPF import filter, follow this procedure:

Note: Before an ACE is modified, it must first be removed from each ACL of which that ACE is a member.

1. In the Import Filters window, click the **ACL** tab. The ACL window appears (Figure 13-4, "RIP/OSPF Import Filters ACL Window").
2. From the Filters column, select the ACL or the row that includes the ACE you wish to modify. Click **Modify**.
3. From the Templates for filter section, select the ACE and using the arrows, move it back to the Pools of all templates section.
4. Click **Ok** to commit or click **Cancel** to exit.
5. Click the **ACE** tab.
6. Select the row that includes the ACE that you wish to modify. Click **Modify**.
7. Modify parameters as necessary.
8. Click **Ok** to commit or click **Cancel** to exit.

Deleting OSPF Import ACEs

Deleting an OSPF Import ACE involves removing the ACE from an ACL within the ACL configuration window, and deleting it as an ACE within the ACE configuration window.

To delete an OSPF ACE follow this procedure:

1. In the Import Filters window, click the **ACL** tab. The ACL window appears (Figure 13-4, “RIP/OSPF Import Filters ACL Window”).
2. Select the row that includes the ACE you wish to delete.
3. Click **Modify**.
4. From the Templates for filter section, select the ACE and using the arrows, move it back to the Pools of all templates section.
5. Click **Ok** to commit or click **Cancel** to exit.
6. Click the **ACE** tab.
7. Select the row that includes the ACE that you wish to delete. Click **Delete**. A confirmation window appears.
8. Click **Yes** to continue or click **Cancel** to exit.

Configuring Import ACLs

An Access Control List (ACL) is a sequential grouping of ACEs that contain the filtering criteria. Before configuring an ACL, you should have configured the ACE's that the ACL will contain .

Before You Begin

Before you begin to create route filters, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **IP** > **IP Routing.**
2. You can configure RIP route filters or OSPF route filters:

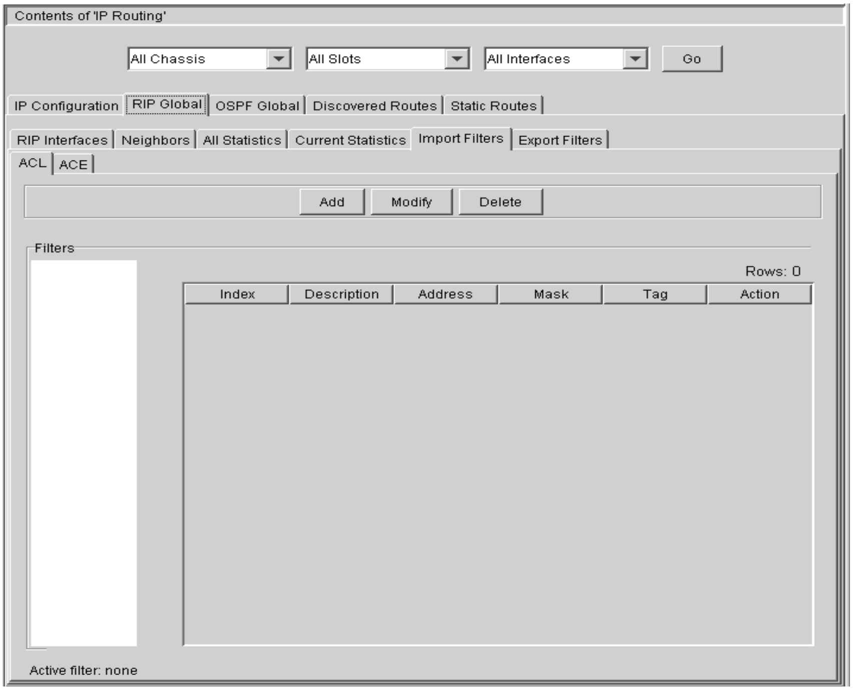
   a To configure the RIP route filters, click the **RIP Global** tab.

   b To configure the OSPF route filters, click the **OSPF Global** tab.
3. Click the **Import Filters** tab.

What You See

This figure is an example of an OSPF Import ACL Add window. This example shows that the new ACL ID # is "1," and that there are two ACEs available to be used for an ACL.

Figure 13-6 Add RIP/OSF Import Filter Window



Understanding ACL Configuration Windows

When you navigate to the ACL windows in the Import and Export ACL tabs, you will see the configuration windows are divided into two sections:

- The left side — Pool of all templates — displays the available ACE pool for creating Import ACLs.
- The right side — Templates for filter — displays the ACEs that are chosen to be used for an ACL. The display is blank when the add box is opened. The ACEs are listed in the section after they are added.

To maneuver between the Pool of all templates and the Templates for filter sections follow this procedure:

- From the Pool of all templates: To move an ACE from the pool and add it for an ACL, select the ACE that you want to move and click on the “>>” button.

- From the Templates for filter**:** To remove an ACE from an ACL and move it back to the ACE pool, select the ACE and click on the **“<<“**button.

Viewing ACE Settings

You may want to view the ACE settings before using it for an ACL. To view the ACE settings, follow this procedure:

1. In the Import Filters window, click the **ACL** tab.
2. Select the ACE from the pool that you wish to view.
3. Click **Details.** A read-only view of that ACE appears.

Sorting ACEs within the ACL

ACEs within the ACL *must be sorted,* in order of the specific-to-general match criteria and action for the ACL. To sort ACEs, follow this procedure:

1. In the Import Filters window, click the **ACL** tab.
2. Select the row that includes the ACE you wish to move from the Templates for filter section.
3. Click **Up** to move the ACE up one level; click **Down** to move the ACE down one level.

Determining ACL Status

Only one ACL can be Active at a time. Activating an ACL automatically deactivates an existing Active ACL.

⚠ ***ACLs must be activated in order for the Cuda 12000 to recognize it during the match process.***

To determine the status of an ACL, follow this procedure:

1. In the Import Filters window, click the ACL tab.
2. View the bottom of the ACL Filters column. The status of the ACL is appears below the Filters column.
    - Active filter: “N” — Indicates that the ACL numbered “N” is activated.

- Active filter: None — Indicates that there are no active filters.

3. Select the ACL ID number that you want to activate, right-click anywhere in the bottom-half of the window and choose **Activate** or **Deactivate.**

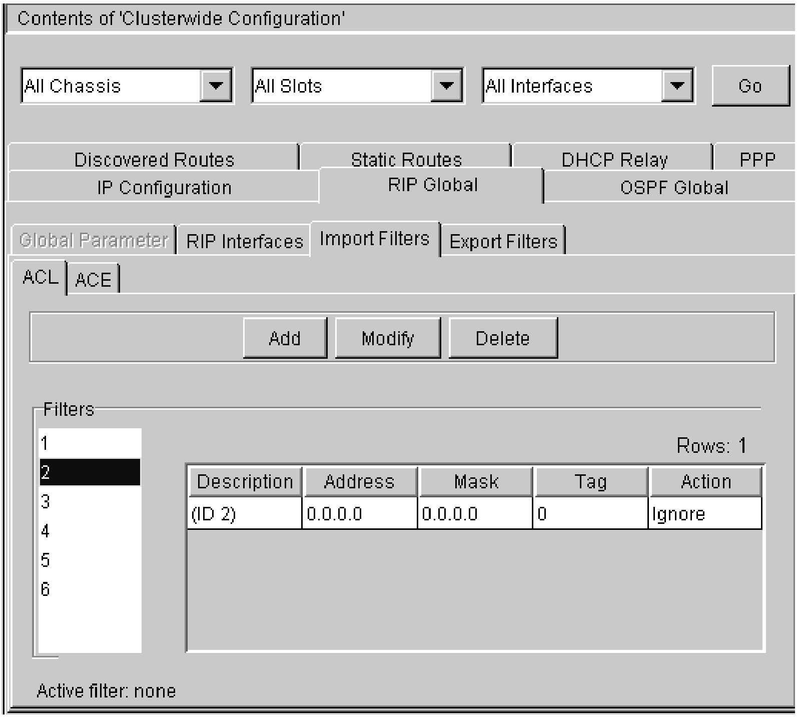
Creating RIP and OSPF Import Filter ACLs

To create RIP and OSPF Import Filter ACLs, follow this procedure:

1. In the Import Filters window, click the **ACE** tab to view an ACE before you add an ACL**.**
2. Click the **ACL** tab.
3. Click **Add**. The Add template list for filter window appears (Figure 13-6, “Add RIP/OSF Import Filter Window”).
4. From the Pool of all templates section, select an ACE for the ACL that you wish to use for the ACL.
5. Using the “>>” toggle button, move the ACE to the Templates for filter section. You may choose more than one ACE for an ACL.
6. If you want to change the filtering order within the ACL, from the Templates for filter section, select the ACE and click **Up** to move the ACE up one level, or click **Down** to move the ACE down one level.
7. After you complete configuration, click **OK** to commit the information or click **Cancel** to exit without saving.

What You See

Figure 13-7 ACL Import Filters Window



Contents of 'Clusterwide Configuration'

All Chassis

All Slots

All Interfaces

Filters

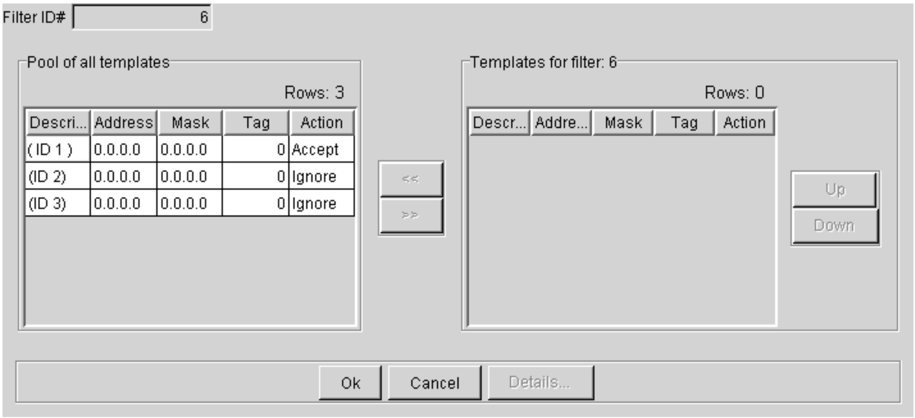
1
2
3
4
5
6

Rows: 1

Description	Address	Mask	Tag	Action
(ID 2)	0.0.0.0	0.0.0.0	0	Ignore

Active filter: none

Figure 13-8 Add template list for filter window.



Filter ID# 6

Pool of all templates

Rows: 3

Descri...	Address	Mask	Tag	Action
(ID 1)	0.0.0.0	0.0.0.0	0	Accept
(ID 2)	0.0.0.0	0.0.0.0	0	Ignore
(ID 3)	0.0.0.0	0.0.0.0	0	Ignore

Templates for filter: 6

Rows: 0

Descr...	Addre...	Mask	Tag	Action

Modifying RIP and OSPF Import Filter ACLs

Modifying Import ACLs involves changing the use of an ACE template. For example, adding an association between an ACE and ACL, or removing an association between an ACE and ACL. In addition, within Modify you may also sort the ACE filtering order. To modify RIP and OSPF Import ACLs, follow this procedure:

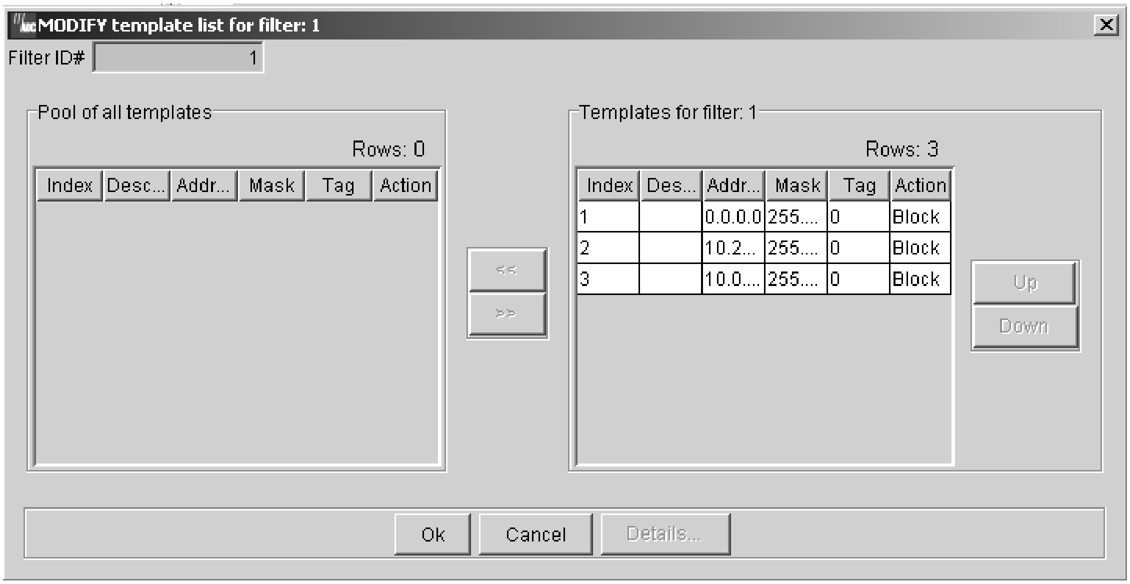
1. In the Import Filters window, click the **ACL** tab.
2. In the Filter column, select the ACL that you wish to modify or select the row that includes the ACE associated with the ACL.
3. Click **Modify**. The MODIFY template list for filter window appears.
4. To view the specifications of an ACE, select the ACE from the Pools of all templates section. Click **Details.**
5. The modification options are:
   - **a** Select an ACE or multiple ACEs from the Pool of all Templates section. Using the ">>" toggle button, move the selected ACE/s to the Templates for filter section.
   - **b** Select an ACE or multiple ACEs from the Templates for filter section. Using the "<<" toggle button, move the ACE/s back to the Pool of all Templates section**.**

c. From the Templates for filter section**,** select an ACE. Using the Up and Down buttons, click Up to move an ACE up one level or click Down to move an ACE down one level.

6. Click **Ok** to commit the modifications or click **Cancel** to exit without saving.

What You See

Figure 13-9 MODIFY Template List for Filter Window



MODIFY template list for filter: 1

Filter ID# 1

Pool of all templates

Rows: 0

Index	Desc...	Addr...	Mask	Tag	Action

Templates for filter: 1

Rows: 3

Index	Des...	Addr...	Mask	Tag	Action
1		0.0.0.0	255....	0	Block
2		10.2...	255....	0	Block
3		10.0....	255....	0	Block

Activating RIP and OSPF Import Filter ACLs

An ACL must be active for the Cuda 12000 to recognize it during the match process. You can only activate one ACL at a time and activating an ACL automatically deactivates an existing active ACL.

To activate or de-activate an ACL, follow this procedure:

1. In the Import Filters window, click the **ACL** tab.
2. Select the RIP or OSPF ACL ID that you want to Activate or Deactivate.
3. Right-click anywhere in the bottom-half of the window and choose **Activate** or **Deactivate.**

Deleting RIP and OSPF Import Filter ACLs

You can delete an ACL when you no longer want to use the list for a route match. To delete Import ACLs follow this procedure:

1. In the Import Filters window, click the **ACL** tab.
2. Select the Filter that you wish to delete.
3. Click **Delete.** A confirmation window appears.
4. Click **Yes** to delete the filter or click **No** to exit without deleting.

Configuring RIP and OSPF Export ACEs

Export ACEs control which routes are advertised to other routers.

RIP and OSPF use route filtering to control the flow of routes to and from routing tables. You use route filtering to increase security, conserve routing table space, or adjust route cost.

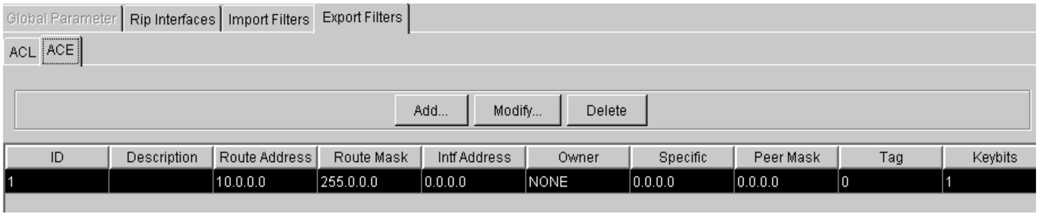
Before You Begin

Before you begin to create export ACEs, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **IP** > **IP Routing.**
2. You can configure RIP route filters or OSPF route filters:
   - **a** To configure the RIP route filters, click the **RIP Global** tab.
   - **b** To configure the OSPF route filters, click the **OSPF Global** tab.
3. Click the **Export Filters** tab.
4. Click the **ACE** tab.

What You See

This figure shows an example of the ACE Export Filters window.



ID	Description	Route Address	Route Mask	Intf Address	Owner	Specific	Peer Mask	Tag	Keybits
1		10.0.0.0	255.0.0.0	0.0.0.0	NONE	0.0.0.0	0.0.0.0	0	1

Creating RIP Export Filter ACEs

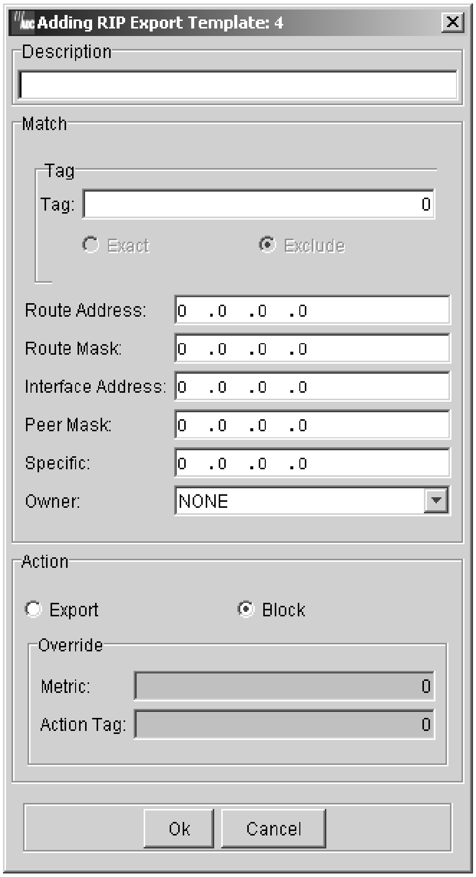
You can create and add RIP Export ACEs to create ACLs to control the advertisement of RIP routes.

Default RIP Export filter ACEs 1, 2, and 3 should not be deleted and replaced with user-defined ACEs. After a power up or reboot, the ACE configuration reverts back to the default templates 1, 2, and 3 configuration that is created upon powering up.

1. In the **ACE** window, click **Add**. The Adding RIP Export Template window appears.
2. Enter values for the parameters.
3. Click **Ok** to commit the information or select **Cancel** to exit.

What You See

Figure 13-10 Adding RIP Export Template Window



Adding RIP Export Template: 4

Description:

Match

Tag

Tag: 0

○ Exact ● Exclude

Route Address: 0 .0 .0 .0

Route Mask: 0 .0 .0 .0

Interface Address: 0 .0 .0 .0

Peer Mask: 0 .0 .0 .0

Specific: 0 .0 .0 .0

Owner: NONE

Action

○ Export ● Block

Override

Metric: 0

Action Tag: 0

Parameter Descriptions

This table provides a description of the Adding RIP Export Template window parameters.

Parameter	Description
Description	Textual description to identify the ACE. The range is 0 to 64 alpha-numeric characters.
Match	Enter values for the match criteria. Any field left blank or set to zero is treated as “don’t care”.
Tag	Match routes on this route tag against routes within the routing database. Choose one of the following two criteria to tag a route: Exact — If the Tag field is specified, then enabling Exact indicates that the match is intended to match all routes with an exact match on the tag field. Exclude — If the Tag field is specified, then enabling Exclude indicates that the match is intended to match all routes that do not match on the tag field.
Route Address	Route Address key to match against routes in the routing database.
Route Mask	Network mask to match against masks for routes in the routing database.
Interface Address	Interface to match against routes in the routing database.
Peer Range Addr	Peer IP address to match against peer routers.
Peer Range Mask	Network mask for the peer routers to match against peer routers.
Specific	A RIP-specific protocol field. Enter the next hop IP address.
Owner	Select the owner of the route. The options are:
NONE	Indicates that the route is not being used as part of the match criteria.
LOCAL	Route for a directly attached network
REMOTE	Static route for a remotely attached network.
SPECIAL	Default route.
OSPF	Route learned through OSPF.
OSPF_EXT	Route learned through OSPF and imported from an external area from a source other than OSPF such as RIP.

Parameter	Description
EGP	Route learned through the External Gateway Protocol*. The Cuda 12000 does not support EGP, in this release*.
BGP_EXT	Route learned through an external BGP router.The Cuda 12000 does not support BGP, in this release.
BGP_INT	The Cuda 12000 does not support BGP internal router, in this release.
Action	Action that you want the system to take when matching outgoing RIP routes. The options are:
Export	Announce the route to be distributed.
Block	Block the route from being distributed.
Override	
Metric	Value overrides the metric value from the routing database entry for this route. Acceptable values are 0-16.
Action Tag	Overrides the tag value from the routing database entry for this route. Acceptable values are listed in the tooltip.

Modifying RIP Export ACEs

Modifying a RIP Import ACE involves removing the ACE from an ACL within the ACL configuration window, and modifying the ACE within the ACE configuration window.

To modify a RIP Export ACE, follow these steps:

1. In the Export Filters window, click the **ACL** tab.
2. Select the row that includes the ACE that you wish to modify.
3. Click **Modify** to open the ACL configuration box.
4. From the Templates for filter section, select the ACE and move it back to the Pools of all templates section.
5. Click **Ok** to commit the changes or click **Cancel** to exit.
6. Click the **ACE** tab.
7. Select the row that includes the ACE that you want to change. Click **Modify.** The Modifying RIP Export Template window appears.
8. Update the information as necessary.
9. Click **OK** to commit the changes or select **Cancel** to exit without saving.

Deleting RIP Export ACEs

Deleting a RIP Export ACE involves removing the ACE from an ACL within the ACL configuration window, and deleting it as an ACE within the ACE configuration window.

To delete a RIP Export ACE follow this procedure:

1. In the Export Filters window, click the **ACL** tab.
2. Select the row that includes the ACE that you wish to delete. Click **Modify**.
3. From the Templates for filter section, select the ACE and move it back to the Pools of all templates section.
4. Click **Ok** to commit the change or click **Cancel** to exit without saving.
5. Click the **ACE** tab.
6. Select the row that includes the ACE that you wish to delete. Click **Delete**. A confirmation window appears.
7. Click **Yes** to continue or click **Cancel** to exit without deleting.

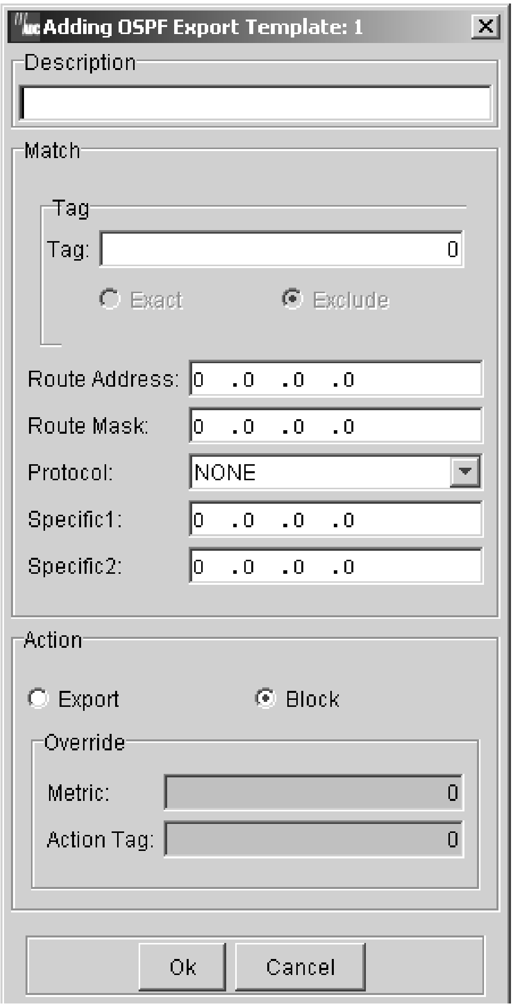
Creating OSPF Export ACEs

This section describes how to create and add OSPF Export ACEs to create ACLs to control the advertisement of OSPF routes.

1. In the Export Filters window, click the **ACE** tab.
2. Click **Add**. The Adding OSPF Export Template window appears.
3. Enter values for the parameters.
4. Click **Ok** to commit the information or click **Cancel** to exit without saving.

What You See

Figure 13-11 Adding OSPF Export Template window.



Adding OSPF Export Template: 1

Description

Match

Tag

Tag: 0

○ Exact ● Exclude

Route Address: 0 .0 .0 .0

Route Mask: 0 .0 .0 .0

Protocol: NONE

Specific1: 0 .0 .0 .0

Specific2: 0 .0 .0 .0

Action

○ Export ● Block

Override

Metric: 0

Action Tag: 0

Parameter Descriptions

This table provides a description of the Adding OSPF Export Template window parameters.

Parameter	Description
Description	Textual description to identify the ACE. The range is 0 to 64 alpha-numeric characters.
Match	Enter values for the match criteria. Any field left blank or set to zero is treated as “don’t care”.

Parameter	Description
Tag	Route tag to match against the value placed in the route tag field of the OSPF packet by the sending router. Exact — If the Tag field is specified, then enabling Exact indicates that the match is intended to match all routes with an exact match on the tag field. Exclude — If the Tag field is specified, then enabling Exclude indicates that the match is intended to match all routes that do not match on the tag field.
Route Address	Route Address key to match against routes in the routing database.
Route Mask	Network mask to match against incoming routes.
Protocol	The options are:
NONE	Indicates that the route is not being used as part of the match criteria.
LOCAL	Route for a directly attached network.
REMOTE	Static route for a remotely attached network.
SPECIAL	Default route.
RIP	Route learned through RIP.
EGP	Route learned through the External Gateway Protocol. *The Cuda 12000 does not support EGP, in this release*.
BGP_EXT	Route learned through an external BGP router.*The Cuda 12000 does not support BGP, in this release*.
BGP_INT	The Cuda 12000 does not support BGP internal router, in this release.
Action	Action that you want the system to take when matching outgoing OSPF routes. The options are:
Specific 1	An OSPF-specific protocol field. Enter the next hop IP address.
Specific 2	An OSPF-specific protocol field. Enter the network IP address.
Action	Action that you want the system to take when matching routes are found. The options are:
Export	Announce the route to be distributed
Block	Block the route from being distributed
Override	The options are:
Metric	Use this value to override the metric value from the routing database entry for this route.

Parameter	Description
Action Tag	Use this value to override the tag value from the routing database entry for this route.

Modifying OSPF Export ACEs

Modifying an OSPF Export ACE involves removing the ACE from an ACL within the ACL configuration window, and modifying the ACE within the ACE configuration window.

To modify an OSPF Export ACE follow this procedure:

1. In the Export Filters window, click the **ACL** tab.
2. Select the row that includes the ACE you wish to modify.
3. Click **Modify**.
4. From the Templates for filter section, select the ACE and move it back to the Pools of all templates section.
5. Click **Ok** to commit the change or click **Cancel** to exit without saving.
6. Click the **ACE** tab.
7. Select the row that includes the ACE that you wish to modify.
8. Click **Modify**. The Modifying OSPF Export Template window appears.
9. Modify parameters as necessary.
10. Click **Ok** to commit the change or click **Cancel** to exit without saving.

Deleting OSPF Export ACEs

Deleting an OSPF Export ACE involves removing the ACE from an ACL within the ACL configuration window, and deleting it as an ACE within the ACE configuration window.

To delete an OSPF Export ACE follow this procedure:

1. In the **Export Filters** window, click the **ACL** tab.
2. Select the row that includes the ACE that you wish to delete. Click **Modify** to open the ACL configuration box.
3. From the Templates for filter section, select the ACE and move it back to the Pools of all templates section.

4. Click **Ok** to commit the change or click **Cancel** to exit without saving.
5. Click the **ACE** tab.
6. Select the row that includes the ACE that you want to delete.
7. Click **Delete** A confirmation window appears.
8. Click **Yes** to continue or click **Cancel** to exit without deleting.

Configuring RIP and OSPF Export ACLs

An ACL is a sequential grouping of ACEs, which contain the filtering criteria. An incoming or outgoing route is compared against all ACEs that comprise the ACL. Whenever a route match is found, the system takes the action that is defined in the ACE.

Configuration involves these functions:

- Creating an ACL by selecting an ACE from a pool and adding it to the ACL.
- Maneuvering ACEs to and from the ACLs.
- Choosing which ACL is to be the Active ACL. ACLs *must be activated* in order for the Cuda 12000 to recognize it during the match process.

Export ACLs control which routes are advertised to other routers. RIP and OSPF use route filters to control the flow of routes to and from routing tables. You may use route filters to increase security, conserve routing table space, or adjust route cost.

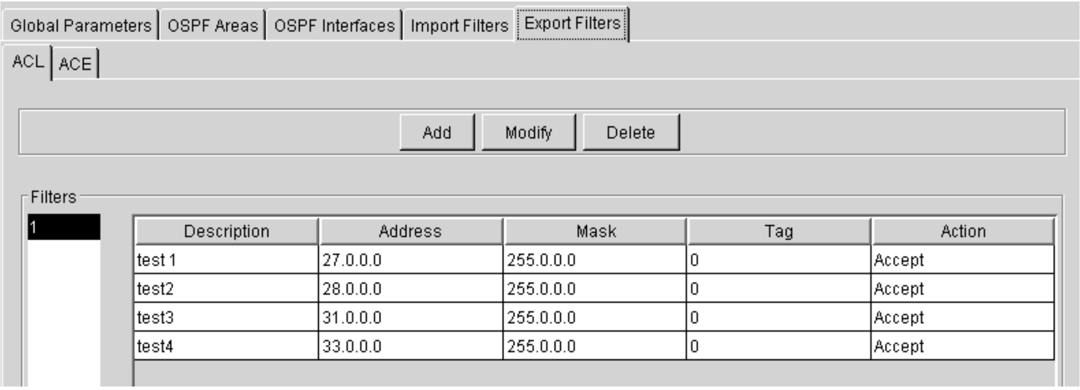
Before You Begin

Before you begin to create export ACLs, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **IP** > **IP Routing.**
2. You can configure RIP route filters or OSPF route filters:
   - **a** To configure the RIP route filters, click the **RIP Global** tab.
   - **b** To configure the OSPF route filters, click the **OSPF Global** tab.
3. Click the **Export Filters** tab.
4. Click the **ACL** tab.

What You See

Figure 13-12 Export Filters ACL Window



Description	Address	Mask	Tag	Action
test 1	27.0.0.0	255.0.0.0	0	Accept
test2	28.0.0.0	255.0.0.0	0	Accept
test3	31.0.0.0	255.0.0.0	0	Accept
test4	33.0.0.0	255.0.0.0	0	Accept

Creating RIP and OSPF Export Filter ACLs

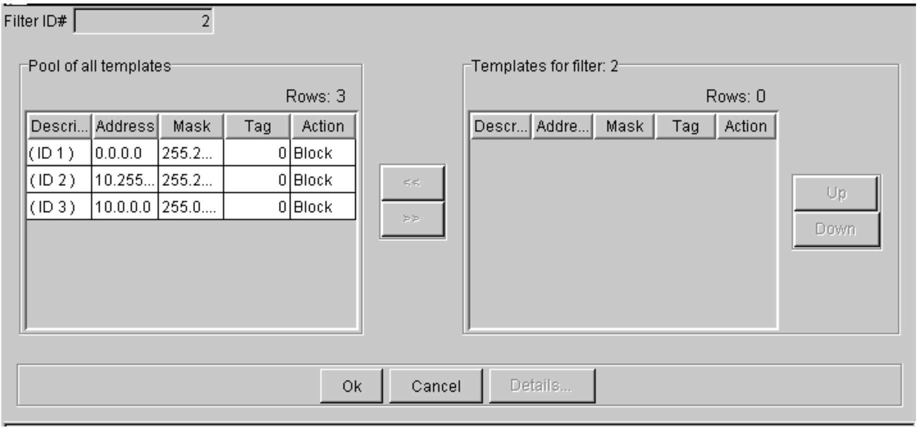
This section describes how to create and add RIP and OSPF Export ACLs. The ACL configuration allows you to create an association between an ACE and ACL.

To create a RIP and OSPF Export ACL follow this procedure:

1. In the Export Filters window, click the **ACE** tab to view the list of ACEs**.**
2. Click the **ACL** tab.
3. Click **Add**. The Add template list for filter window appears.
4. To select an ACE to associate with the ACL, select the ACE that you want to use from the Pool of all templates section
5. Using the “>>” toggle button, move the ACE to the Templates for filter section. You may choose more than one ACE for an ACL.
6. If you associated multiple ACEs and want to change the filtering order, from the Templates for filter section, select the ACE. Using the Up and Down buttons click **Up** to move the ACE up one level, or click **Down** to move the ACE down one level.
7. Click **Ok** to commit the changes or click **Cancel** to exit without saving.

What You See

Adding Template List for Filter Window



Filter ID# 2

Pool of all templates

Rows: 3

Descri...	Address	Mask	Tag	Action
(ID 1)	0.0.0.0	255.2...	0	Block
(ID 2)	10.255...	255.2...	0	Block
(ID 3)	10.0.0.0	255.0....	0	Block

Templates for filter: 2

Rows: 0

Descr...	Addre...	Mask	Tag	Action

Modifying RIP and OSPF Export Filter ACLs

Modifying Export ACLs involves changing the use of an ACE. For example, adding and association between an ACE and an ACL, or removing an association between an ACE and an ACL. You may sort the ACE filtering order.

To modify an export filter ACL, follow this procedure:

1. In the **ACL** window, select the ACL or the row that includes the ACL that you wish to modify in the Filter column.
2. Click **Modify.** The MODIFY template list for filter window appears.
3. To view the specifications of an ACE before you change it, select the ACE from the Pools of all templates section.
4. Click **Details**.
5. The modification options are:

   a Associate ACEs to ACL — Select an ACE or multiple ACEs from the Pool of all Templates section. Using the ">>" toggle button, move the selected ACE/s to the Templates for filter section.

   b Remove Association between ACEs and ACLs— Select an ACE or multiple ACEs from the Templates for filter section. Using the "<<"

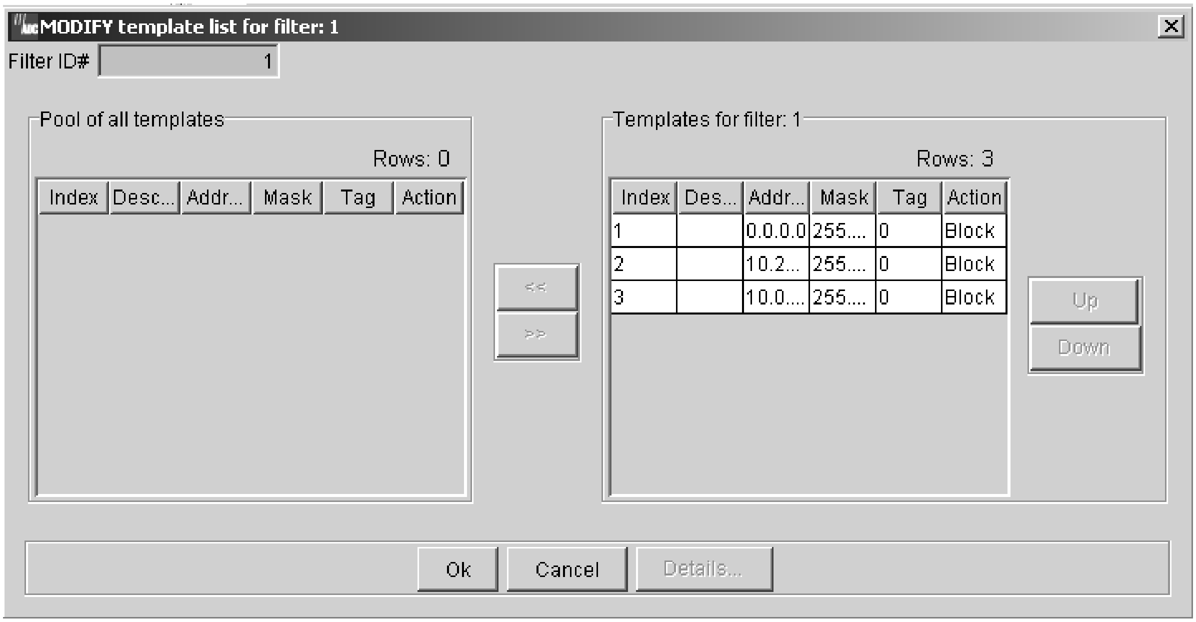
toggle button, move the ACE/s back to the Pool of all Templates section.

c Sort ACEs Filtering Order— From the Templates for filter section, select an ACE. Using the Up and Down options click **Up** to move an ACE up one level or click **Down** to move an ACE down one level.

6. Click **Ok** to commit the changes or click **Cancel** to exit without saving.

What You See

Figure 13-13 Modify Template List for Filter Window.



MODIFY template list for filter: 1

Filter ID# 1

Pool of all templates

Rows: 0

Index	Desc...	Addr...	Mask	Tag	Action

Templates for filter: 1

Rows: 3

Index	Des...	Addr...	Mask	Tag	Action
1		0.0.0.0	255....	0	Block
2		10.2...	255....	0	Block
3		10.0....	255....	0	Block

Activating RIP and OSPF Export Filter ACLs

An ACL must be activated in order for the Cuda 12000 to recognize it during the match process. You can only activate one filter at a time and activating a filter automatically deactivates an existing active filter.

To activate an export filter ACL, follow this procedure:

1. In the ACL window, select the filter you wish to activate or deactivate.
2. Right-click anywhere on the bottom-half of the window and select **Activate** or **Deactivate**.

Deleting RIP and OSPF Export Filter ACLs

You delete an ACL when you no longer want to use the list for a route match. To delete Export ACLs follow this procedure:

3. In the ACL window, select the ACL you wish to delete from the Filters column.
4. Click **Delete.** A confirmation window appears.
5. Click **Yes** to continue or choose **No** to exit without deleting.

14 IP PACKET FILTERING

This chapter describes IP packet filtering on the Cuda 12000 and includes:

- About IP Packet Filtering
- Enabling and Disabling IP Packet Filtering
- Access Lists
- Applying Access Lists to Interfaces
- Enabling and Disabling IP Filter Aging
- Packet Filtering Considerations

IP packet filtering is only supported on cable interfaces.

About IP Packet Filtering

The Cuda 12000 supports packet filtering in the form of access lists. Access lists allow you to restrict and control IP packet flow over specified cable interfaces. This control of IP packet transmission restricts network access from specified users, devices, and applications. IP packet filtering involves:

- Creating access lists to define the IP packet filtering criteria.
- Applying the access lists to specified interfaces.
- Enabling IP packet filtering on specified interfaces.

Before You Begin

Before you configure IP Packet Filtering, navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **IP** > **IP Packet Filtering**

Enabling and Disabling IP Packet Filtering

When you apply an access-list to an interface, IP filtering is automatically enabled. For each interface, you can enable filtering on incoming and outgoing packets.

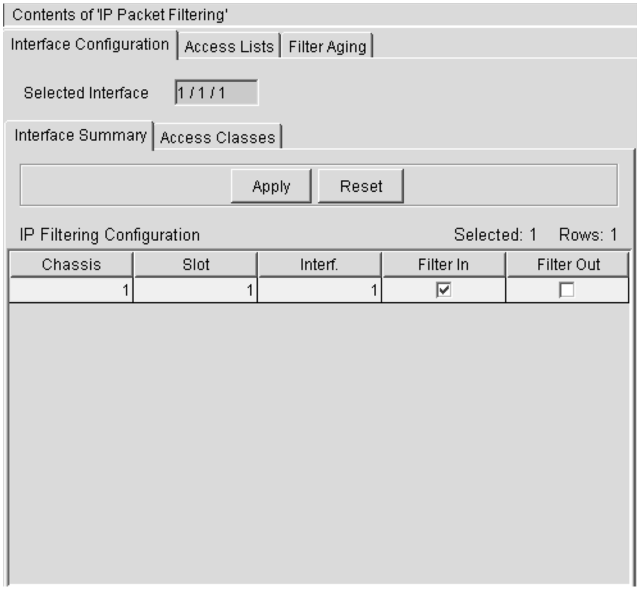
Disabling IP filtering means that all packets are permitted to cross the interface. IP filtering is *not* automatically disabled when access lists are removed. You must disable access lists manually.

To enable or disable IP filtering, follow this procedure:

1. In the IP Packet Filtering window, click the **Interface Configuration** tab.
2. Click the **Interface Summary** tab. The Interface Summary window appears.
3. Select the row that includes the interface you wish to enable or disable for IP Packet Filtering.
4. Select or clear the **Filter In** or **Filter Out** check boxes to enable or disable IP Packet Filtering.
5. Click **Apply** to commit the changes or click **Reset** to return the parameters to the previous values.

What You See

Figure 14-1 IP Packet Filter Interface Summary Window



Selected Interface 1 / 1 / 1

IP Filtering Configuration Selected: 1 Rows: 1

Chassis	Slot	Interf.	Filter In	Filter Out
1	1	1	☑	□

Access Lists

Access lists are sequential groupings of permit and deny rules. These rules enable you to permit or deny packets from crossing specified interfaces. An access list is comprised of rules containing both match criteria and actions to take upon finding a match.

Match criteria can include:

- Source IP address and mask
- Destination IP address and mask
- Source TCP/UDP port range
- Destination TCP/UDP port range
- TCP Sync Flag
- TCP Establish State
- IP Type of Service (TOS) and mask

Actions that can be taken against matching packets include:

- Permit
- Deny
- Change IP TOS

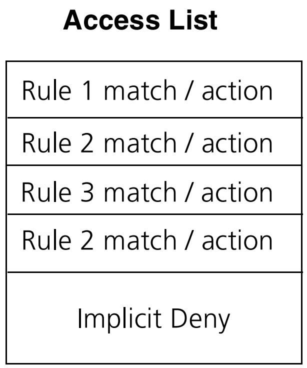
Access lists are pooled and indexed on a chassis-wide basis. Access lists are then only used by an interface when you enable IP filtering on the interface and apply the predefined access-lists to the interface. Each access-list is identified by a list number that you define when creating the list.

Access lists are comprised of rules that are sequenced according to assigned rule numbers. Packets are then matched against the lowest numbered rules first.

Each rule defines a permit or deny action which determines whether the packet is accepted or permitted when matched. Access lists include an implicit deny command at the end. This means that an IP filter-enabled interface rejects (drops) packets for which no match is found.

Figure 14-2 shows a logical representation of an access list:

Figure 14-2 Access List



You can use access lists to filter these protocols:

- Internet Protocol (IP)
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)

When masking network addresses, 0 indicates "care" bits; 1 indicates "don't care." For example, a class C network would be masked as 0.0.0.255.

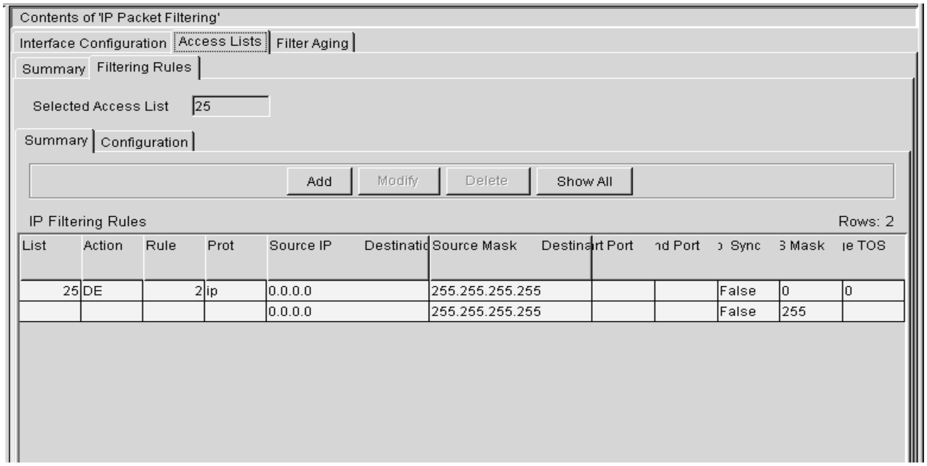
Before You Begin

Before you configure Access Lists, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **IP** > **IP Packet Filtering.**
2. Click the **Access Lists** tab. The Access List window appears.
3. Navigate through the **Access Lists** tab structure to **Filtering Rules** > **Summary**. The Summary window appears.

What You See

Figure 14-3 Filtering Rules Summary Window



Contents of 'IP Packet Filtering'

Selected Access List 25

IP Filtering Rules Rows: 2

List	Action	Rule	Prot	Source IP	Destinatic	Source Mask	Destina	rt Port	ıd Port	ɔ Sync	3 Mask	ıe TOS
25	DE	2	ip	0.0.0.0		255.255.255.255				False	0	0
				0.0.0.0		255.255.255.255				False	255	

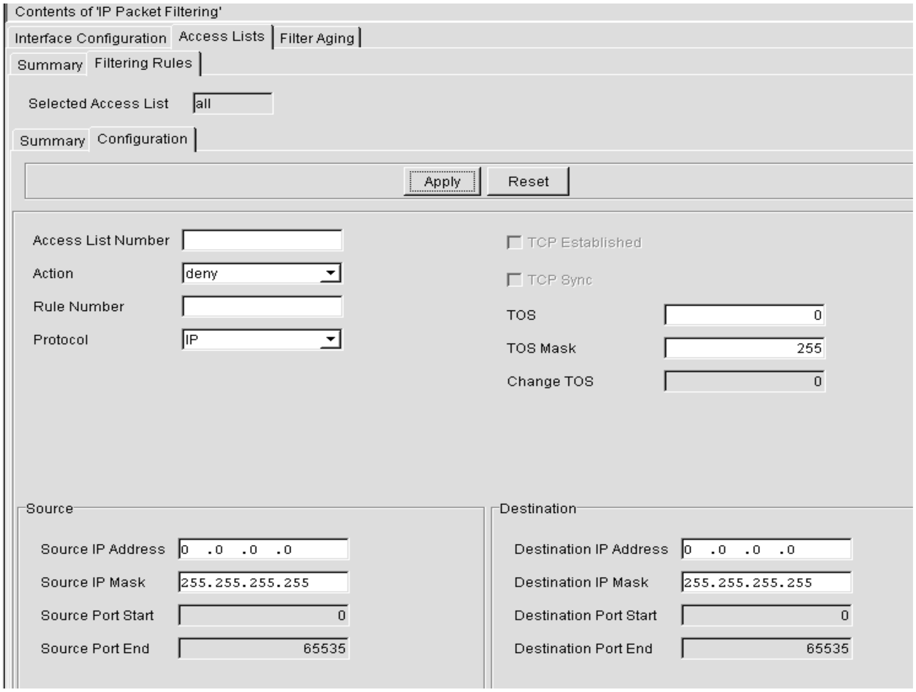
Creating Access Lists

To create access lists, follow this procedure:

1. In the Filtering Rules window, click the **Configuration** tab. The Configuration window appears.
2. Enter values for the parameters. Refer to Table 14-1.
3. Click **Apply** to commit the changes or **Reset** to reload the default values.

What You See

Figure 14-4 Filtering Rules Configuration Window (Two Screens)



Contents of 'IP Packet Filtering'

Selected Access List: all

Access List Number:
Action: deny
Rule Number:
Protocol: IP

□ TCP Established
□ TCP Sync
TOS: 0
TOS Mask: 255
Change TOS: 0

Source IP Address: 0 .0 .0 .0
Source IP Mask: 255.255.255.255
Source Port Start: 0
Source Port End: 65535

Destination IP Address: 0 .0 .0 .0
Destination IP Mask: 255.255.255.255
Destination Port Start: 0
Destination Port End: 65535

Parameter Descriptions

This table provides a description of the Filtering Rules Configuration window.

Table 14-1 Filtering Rules Parameters

Parameter	Description
Access List Number	Index number that identifies the access list. Valid range 1 - 16384.
Action	Action to be taken against matching packets including Deny, Permit, or Change TOS. The default is Deny.
Rule Number	Number identifying the precedence of this rule within the access list. Smaller rule numbers result in greater precedence. This means that rules are processed from lower to higher rule numbers.

Parameter	Description
Protocol	Protocol that you want the rule to filter including IP, TCP, or UDP.
TCP Established	Indicates an established TCP connection. A match occurs when the ACK or RST bits of a TCP datagram are set. The default is false.
TCP Sync	Indicates a match on the TCP SYNC flag.
TOS	Type of Service (TOS) level identified in the IP packet header. Valid range 0 - 255.
TOS Mask	Type of Service (TOS) mask. Valid range 0 - 255.
Change TOS	Change the TOS value. Valid range 0 - 255.
Source	The options are:
Source IP Address	IP address seen in the source IP address field of the protocol header.
Source IP Mask	Source IP address network mask, if you specified a specific address or 255.255.255.255 to indicate a match on "Any" packet.
Source Port Start	Start of the TCP or UDP source port range in which to filter. Valid range 0 - 65535.
Source Port End	End of the TCP or UDP source port range in which to filter. Valid range 0 - 65535
Destination	The options are:
Destination IP Address	IP address seen in the destination IP address field of the protocol header.
Destination IP Mask	Destination IP address network mask, if you specified a specific address or 255.255.255.255 to indicate a match on "Any" packet.
Destination Port Start	Start of the TCP or UDP destination port range in which to filter. Valid range 0 - 65535.
Destination Port End	End of the TCP or UDP destination port range in which to filter. Valid range 0 - 65535.

Modifying Access Lists

To modify an access list, follow this procedure:

1. In the Summary window, select the list you wish to modify.
2. Click **Modify**. The Configuration window appears.
3. Modify the desired parameters. Refer to Table 14-1.
4. Click **Apply** to commit the information or click **Cancel**.

Deleting Access Lists

1. In the Summary window, select the list you want to delete.
2. Click **Delete**. A confirmation window appears.
3. Click **Ok** to continue or click **Cancel**.

Applying Access Lists to Interfaces

After you create an access list, you can apply it to one or more CMTS interface to filter traffic. Filters can be applied to either outbound or inbound interfaces or both.

Filtering is enabled automatically when you apply an access list to an interface. When filtering is enabled with no access lists applied to the interface, the interface permits all traffic to pass.

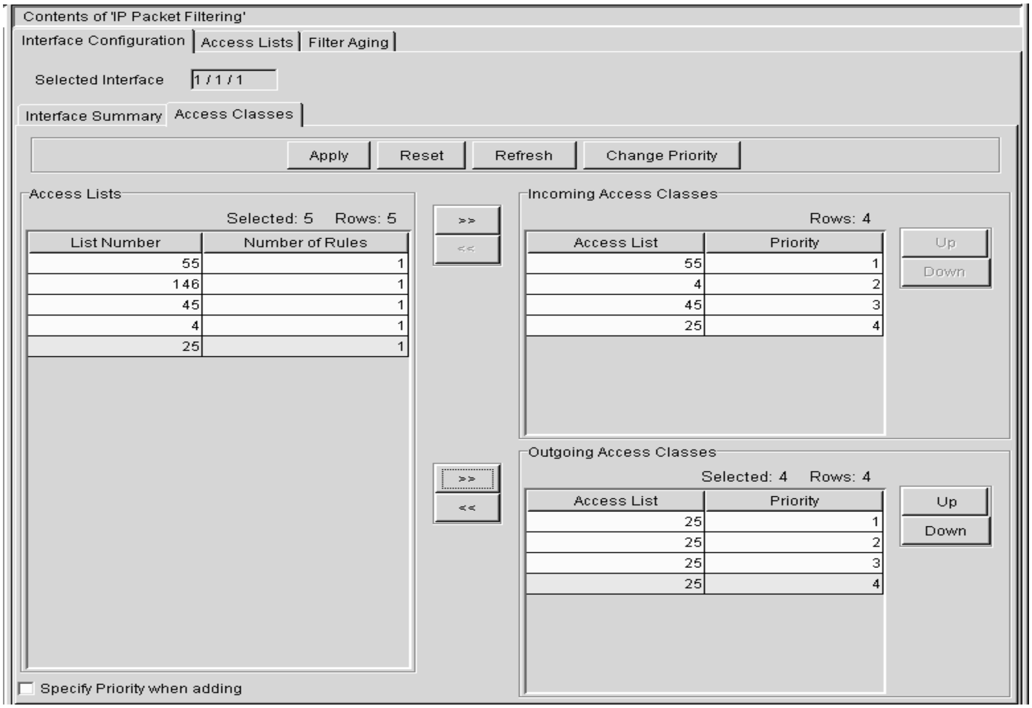
Before You Begin

Before you configure Access Lists, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **IP** > **IP Packet Filtering.**
2. Click the **Interface Configuration** tab. The Interface Configuration window appears.
3. Select an interface.
4. Click the **Access Classes** tab. The Access Classes window appears.
5. Click **Refresh** to update the information.

What You See

Figure 14-5 Access Classes Window



Selected Interface 1 / 1 / 1

Access Lists

Selected: 5 Rows: 5

List Number	Number of Rules
55	1
146	1
45	1
4	1
25	1

Incoming Access Classes

Rows: 4

Access List	Priority
55	1
4	2
45	3
25	4

Outgoing Access Classes

Selected: 4 Rows: 4

Access List	Priority
25	1
25	2
25	3
25	4

□ Specify Priority when adding

Parameter Descriptions

This table provides a description of the Access Classes window

Table 14-2 Access Classes Parameters.

Parameter	Description
Access Lists	
List Number	Index number that identifies the list
Number of Rules	Number of rules in a list
Incoming Access Classes	
Access List	Index number that identifies the list.

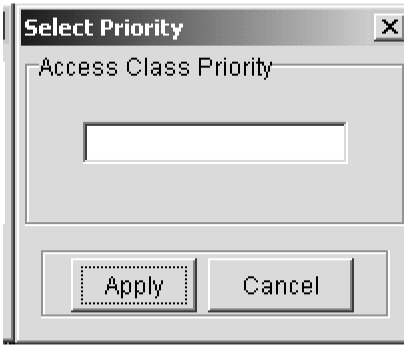
Parameter	Description
Priority	Specifies the order of access list examination within the access class.
Outgoing Access Classes	
Access List	Index number that identifies the list.
Priority	Specifies the order of access list examination within the access class.
Specify Priority When Adding	When selected, results in the Select Priority window to display when you are applying an access list to an interface. If not selected, refer to the Changing the Priority section.

Applying Access Lists

To apply an access list to an interface, follow this procedure:

1. In the Access Lists window, select a row in the Access Lists table that includes the list you wish to apply to an incoming or outgoing interface.
2. If you want to specify a priority for the access list, select the **Specify Priority When Adding** option.
3. Click the arrow button to move the row to the incoming or outgoing interface, or both. If you did not choose to specify a priority, go to step 5.
4. If you chose to specify a priority (step 2), the **Select Priority** window appears (Figure 14-6). Enter the priority and click **Apply**.
5. In the Access Classes window, click **Apply** to commit the changes or click **Reset** to return the parameters to the reset values.

Figure 14-6 Select Priority Window



Changing the Priority

Just as the rule number determines the sequence of rule examination within an access list, *priority* specifies the order of access list examination within the access class that you apply to an inbound or outbound interface.

Figure 14-7 shows a logical representation of an access class for an inbound or outbound interface.

Figure 14-7 Access Class

Access Class/Inbound	Access Class/Outbound
Access List 1 / Priority 1	Access List 1 / Priority 1
Access List 2 / Priority 2	Access List 2 / Priority 2
Access List 3 / Priority 3	Access List 3 / Priority 3
Access List 4 / Priority 4	Access List 4 / Priority 4
Access List 5 / Priority 5	Access List 5 / Priority 5

To change the priority of an access class, follow this procedures:

1. In the Incoming and/or Outgoing Access Classes window, select the list for which you wish to change the priority in the Incoming Access Classes or Outgoing Access Classes window.
2. Click **Change Priority.** The Select Priority window appears.

3. Enter the new priority in the Access Class Priority field.
4. Click **Apply** to commit the change or click **Cancel** to exit without saving.
5. In the Access Classes window, click **Apply** to commit the changes or click **Reset** to return the parameters to the reset values.

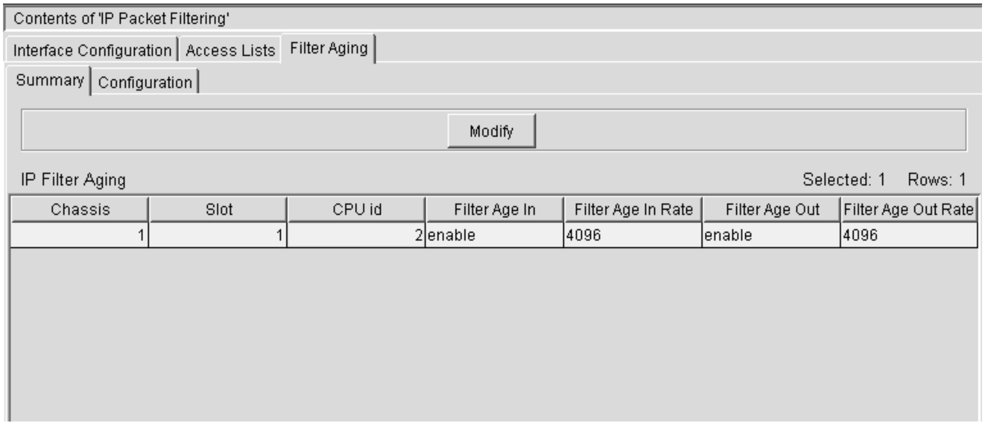
Enabling or Disabling IP Filter Aging

When you enable IP Filter Aging on a particular interface, the filter flow table is periodically examined for activity at a computed rate. If a flow shows no activity during an examination period, the flow is removed from the table.

To enable or disable IP Filter Aging, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **IP** > **IP Packet Filtering**.
2. Click the **Filter Aging** tab. The Filter Aging Summary window appears (Figure 14-8, "Filter Aging Summary Window").
3. Select the row that includes the interface for which you want to enable or disable IP Filtering. The Configuration window appears (Figure 14-9,"Filter Aging Configuration Window").
4. Enter values for the Filter Age In and Filter Age Out parameters. Refer to Table 14-4.
5. Click **Apply** to commit the changes or Click **Reset** to reset the parameters.

Figure 14-8 Filter Aging Summary Window



Chassis	Slot	CPU id	Filter Age In	Filter Age In Rate	Filter Age Out	Filter Age Out Rate
1	1	2	enable	4096	enable	4096

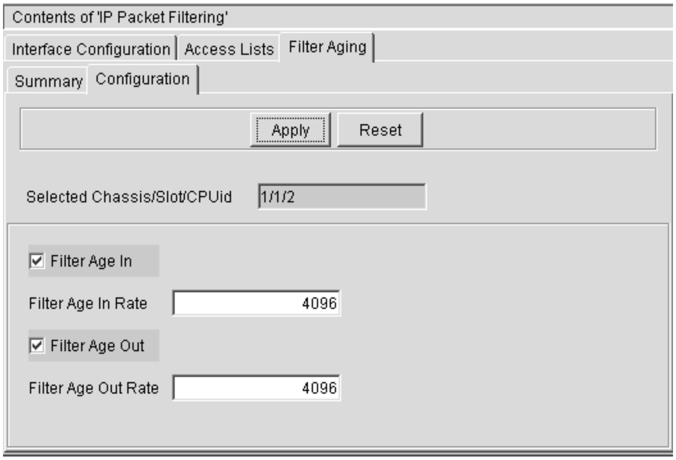
Parameter Descriptions

This table provides a description of the Filter Aging Summary window.

Table 14-3 Filter Aging Summary Parameters

Parameter	Description
Chassis ID	Unique identification number you assign to a Cuda 12000 chassis in the network. The Cuda uses a multi-range numbering system. Acceptable chassis ID values are 1 to 128. The Cuda defaults with chassis number 255. We recommend that you do not change the chassis ID. This may cause the Cuda 12000 to lose the configuration that is saved on the provisioning database, as well as other persisted files.
Slot	Indicates the slot number in which the Primary management module is located.
CPU ID	ID of the CPU.
Filter Age In	All inbound interfaces within the current slot number.
Filter Age In Rate	Filter aging rate in seconds. Sets the number of seconds before a flow (flow table entry) is aged out (removed) for inbound traffic interfaces.
Filter Age Out	All outbound interfaces within the current slot.
Filter Age Out Rate	Filter aging rate in seconds. Sets the number of seconds before a flow (flow table entry) is aged out (removed) for outbound traffic interfaces.

Figure 14-9 Filter Aging Configuration Window



Selected Chassis/Slot/CPUid 1/1/2

☑ Filter Age In

Filter Age In Rate 4096

☑ Filter Age Out

Filter Age Out Rate 4096

Parameter Descriptions

This table provides a description of the Filter Aging Configuration window

Table 14-4 Filter Aging Configuration Parameters.

Parameter	Description
Filter Age In	Select or deselect the Filter Age In check box to enable or disable IP Filter Age In
Filter Age In Rate	Indicates the flow aging rate, in flows/second, when Flow Age In is enabled. The valid range is 400 - 4096 flows/second. The default is 4096, which means the entire flow table can be examined in 16 seconds.
Filter Age Out	Select or deselect the check box to enable or disable IP FIlter Age In.
Filter Age Out Rate	Indicates the flow aging rate, in flow/second, when Flow Age Out is enabled. The valid range is 400 - 4096 flows/second. The default is 4096, which means the entire flow table can be examined in 16 seconds.

Modifying IP Filter Aging

To modify the IP Filter Aging for an interface follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **IP** > **IP Packet Filtering.**
2. Click the **Filter Aging** tab.
3. Click the **Summary** tab. The Filter Aging Summary window appears (Figure 14-8, “Filter Aging Summary Window”).
4. Select the row that includes the interface you want to modify.
5. Click **Modify**. The Configuration window appears (Figure 14-9,“Filter Aging Configuration Window”).
6. Modify the required parameters. Refer to Table 14-4.
7. Click **Apply** to commit the changes or click **Reset** to reset the parameters.

Packet Filtering Considerations

When creating packet filters, consider these points:

- Access lists contain an implicit deny at the end. This means packets for which no match is found are rejected. When more than one access list is applied to an interface, non-matching packets are compared to the access-list with the next highest priority. If a match is still not found, the packet is matched against the next access list. If, after applying the packet to the final access list on an interface, a match is not found the packet is dropped.
- The sequence in which an inbound or outbound packet is matched against the filter criteria of an interface is determined by the following:
  - Rule number within access list — Lower rule numbers take precedence over higher rule numbers. This means that within an access list, the rule with the lower number is examined first.
  - Priority of access-list within the access class — When you apply an access-list to an interface, access lists assigned lower priorities take precedence over lists assigned higher priorities. This means that within an access class, the access list with the lower number is examined first.

15 NETWORK-LAYER BRIDGING

Network-layer bridging allows a single subnet to span across multiple DOCSIS modules. This chapter provides information and procedures about network-layer bridging on the Cuda 12000 and includes the following sections:

- About Network-Layer Bridging
- Creating Network-Layer Bridges
- Creating Bridge Groups
- Adding Interfaces to Bridge Groups
- Assigning IP Addresses to Bridge Groups
- Assigning Bridged Interfaces to Gateways
- Setting Bridge Flow Timers

About Network-Layer Bridging

Network-layer bridging allows you to add the same IP address to multiple physical interfaces throughout the system. Of particular value is the ability to propagate the same IP gateway across cable interfaces on multiple DOCSIS (CMTS) modules.

The cable modem, customer premise equipment (CPE), or Multimedia Terminal Adapter (MTA) gateway determines the subnet to which a modem, CPE, or MTA can belong. When the provisioning server receives a DHCP request from a cable modem, CPE device, or MTA, it uses the cable modem, CPE, or MTA gateway as a key to determine from which subnet or subnet pool to assign an address. For more information about provisioning, refer to the *FastFlow Broadband Provisioning Manager GUI-based Administration Guide*, or the documentation for your third-party provisioning manager.

Routing logic dictates that each interface in the system must have a unique IP address. Network-layer bridging support allows you to group multiple interfaces residing on multiple modules into a single logical interface, known as a *bridge group.* After you assign an IP address to this bridge group, the address will apply to all interfaces that are members of the bridge group.

Creating Network-Layer Bridges

The key to spanning a single subnet across multiple DOCSIS modules is to configure the same IP gateway on each module. The gateway serves as the key that dictates address assignment for cable modems and CPE devices, as a result, configuring the same IP gateway on each cable interface enables the DHCP server to assign those devices IP addresses from the same subnet or subnet pool.

This means that cable modems attached to a DOCSIS module in slot 1 can belong to the same subnet as the cable modems attached to a DOCSIS module in slot 8. You can then physically move modems between DOCSIS modules without assigning new addresses; the shift of cable modems between modules becomes plug and play.

To span a subnet across multiple cable interfaces, perform the following steps. These steps are described in the appropriate sections that follow:

1. Create a bridge group.
2. Add the interfaces on which you want to install the same gateway to the bridge group.
3. Assign the IP address that you want to use as the cable modem, CPE, and MTA gateway to the bridge group. Note that the address that you assign to the bridge group is automatically added to the routing table.
4. Configure the DHCP relay agent on each cable interface so that the IP address is configured as the cable modem, CPE, and/or MTA gateway.

The system supports network-layer bridging within a single chassis where egress ports within the chassis share an IP address. It also supports network-layer bridging within a cluster where egress ports on modules that reside in different chassis can share an IP address. In this way, the layer 3 bridge can span across a single chassis, or multiple chassis in the same cluster.

If for any reason you would like to assign the same IP address for non-cable interfaces, note that you can also add Ethernet and Gigabit Ethernet interfaces to bridge groups.

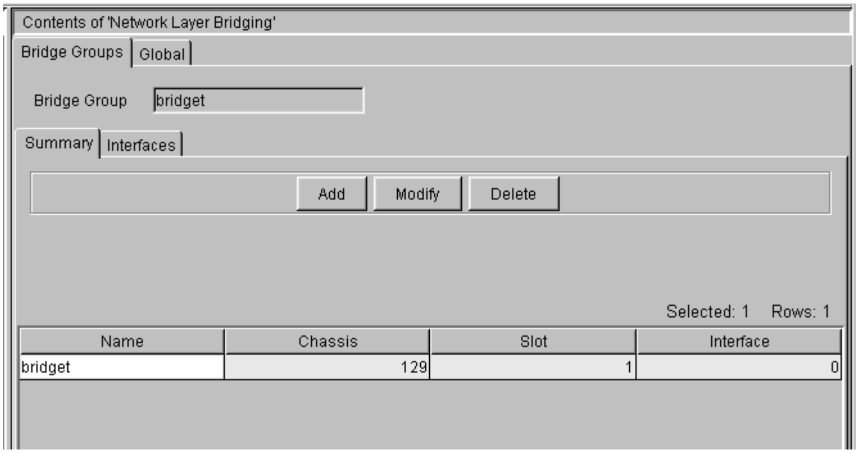
- POS interfaces cannot be added to a network-layer bridge.
- You may assign multiple IP addresses to a specified bridge group.
- A single egress port can belong to a maximum of 16 different NLBGs.
- An NLBG can contain up to 32 physical interfaces; you can define a maximum of 16 NLBGs on single chassis.

Before You Begin

Before you create network-layer bridges, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **IP** > **Network Layer Bridging**.
2. Click the **Summary** tab. The Summary window appears.

Figure 15-1 Network Layer Bridging Summary Window



Bridge Group: bridget

Selected: 1 Rows: 1

Name	Chassis	Slot	Interface
bridget	129	1	0

Table 15-1 Summary Window Parameters

Parameter	**Description**
Name	The name of this network layer bridge group.
Chassis	Specifies the chassis ID of the NLBG group in the network. The Cuda 12000 assigns chassis number 129 to all NLBG groups.
Slot	Specifies the slot for the NLBG group. The Cuda 12000 assigns slot number 1 to all NLBG groups.
Interface	Interface ID of the NLBG group. The Interface ID corresponds to the NLBG group number. Acceptable values are 1 to 15.

Creating Bridge Groups

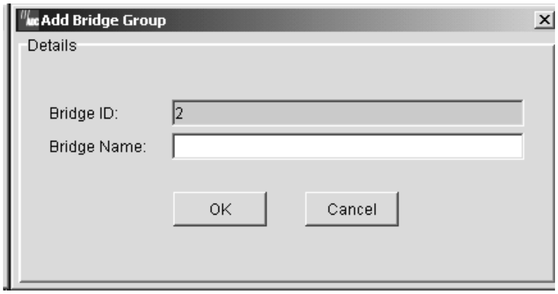
You must first create a network-layer bridge group before you can configure it.

To create a bridge group, follow this procedure:

1. In the Network Layer Bridging Summary window, click **Add**. The Add Bridge Group window appears.
2. Enter a name for the bridge group. Refer to Table 15-2. Click **Ok** to commit the entry or **Cancel** to exit without saving.

What You See

Figure 15-2 Add Bridge Group Window



Bridge ID: 2

Bridge Name:

Table 15-2 Add Bridge Group Window Parameters

Parameter	Description
Bridge ID	Number assigned to network layer bridge group.
Bridge Name	The name of this network layer bridge group.

Deleting Bridge Groups

To delete a bridge group, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **IP** > **Network Layer Bridging**.
2. In the Network Layer Bridging Summary window, select the Bridge Group you wish to delete.
3. Click **Delete**. A confirmation window appears.

4. Click **Yes** to delete the group or click **No** to exit without deleting.

Adding Interfaces to Bridge Groups

After you create a bridge group, you can assign system interfaces to it. All interfaces that you add to the bridge group become part of the layer 3 bridge.

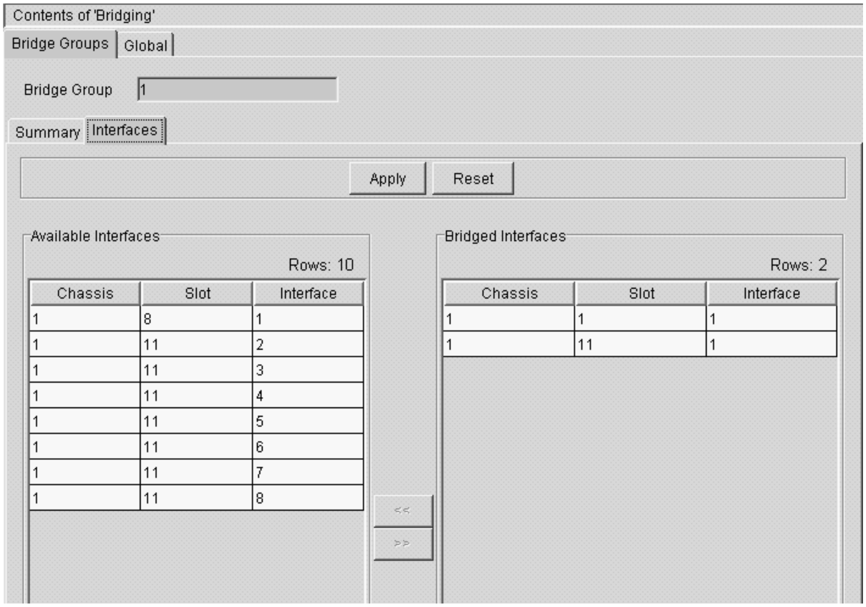
To add interfaces to a bridge group, follow this procedure:

1. In the Summary window, select the group in which you want to add the interface.
2. Click the **Interfaces** tab.
3. In the Available Interfaces table, select the row that includes the interface that you wish to apply to the bridged interface.
4. Click the arrow to move the row to the Bridged Interfaces table.
5. Click **Apply** to commit the changes or click **Reset** to return to the previous values.

What You See

This figure shows an example of the Bridge Group Interfaces window.

Figure 15-3 Bridge Group Interfaces Window



Bridge Group: 1

Available Interfaces

Rows: 10

Chassis	Slot	Interface
1	8	1
1	11	2
1	11	3
1	11	4
1	11	5
1	11	6
1	11	7
1	11	8

Bridged Interfaces

Rows: 2

Chassis	Slot	Interface
1	1	1
1	11	1

Parameters

This table describes the parameters of the Bridge Group Interfaces window.

Table 15-3 Bridge Group Interfaces Parameters

Parameter	Description
Chassis ID	Specifies the new chassis ID for this Cuda 12000 in the network. The Cuda 12000 uses a multi-range numbering system. Acceptable chassis ID values are 1 to 128, or 255. The default is one.
Slot	This indicates the slot in which the Management module is installed.
Interface	Interface ID of the Route Server module.

Assigning IP Addresses to Bridge Groups

A network-layer bridge is comprised of interfaces that belong to the same bridge group. They share any IP address that you assign to the bridge group. The IP address that you assign to the bridge-group is automatically added to the routing table.

Note that because the routing table is automatically updated upon assigning the IP address to the bridge group, you do not have to specifically install the address on the physical interface.

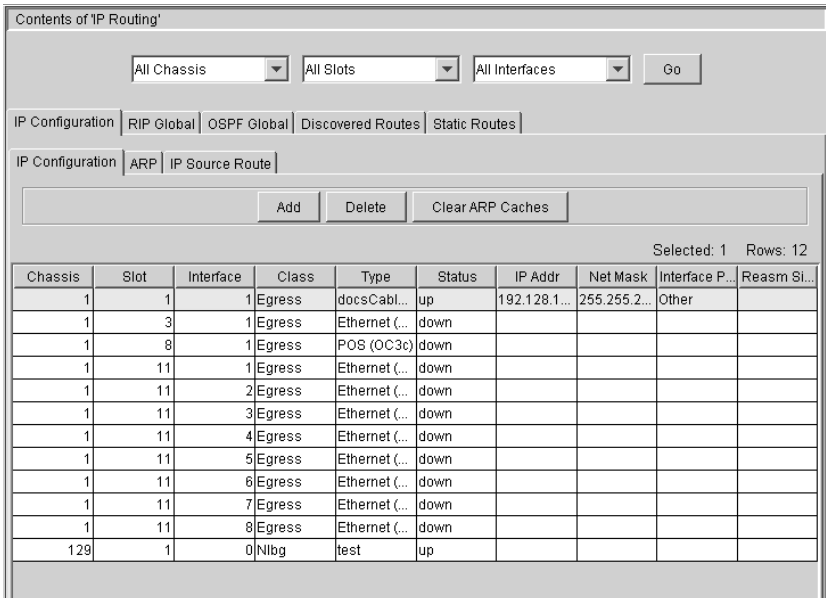
You assign an IP address to a network-layer bridge just as you would any physical interface. For more information about assigning IP addresses to physical interfaces, refer to Chapter 12, “Configuring IP Routing”.

To assign an IP address to a bridge group, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **IP** > **IP Routing.**
2. Click the **IP Configuration** tab.
3. Click the **IP Configuration** sub tab. The IP Configuration window appears.
4. Select the row that includes the bridge group to which you want to assign an IP address. The bridge group is identified as Nlbg in the Class column.

What You See

Figure 15-4 IP Configuration Window



Selected: 1 Rows: 12

Chassis	Slot	Interface	Class	Type	Status	IP Addr	Net Mask	Interface P...	Reasm Si...
1	1	1	Egress	docsCabl...	up	192.128.1...	255.255.2...	Other	
1	3	1	Egress	Ethernet (...	down				
1	8	1	Egress	POS (OC3c)	down				
1	11	1	Egress	Ethernet (...	down				
1	11	2	Egress	Ethernet (...	down				
1	11	3	Egress	Ethernet (...	down				
1	11	4	Egress	Ethernet (...	down				
1	11	5	Egress	Ethernet (...	down				
1	11	6	Egress	Ethernet (...	down				
1	11	7	Egress	Ethernet (...	down				
1	11	8	Egress	Ethernet (...	down				
129	1	0	Nlbg	test	up				

Parameter Descriptions

This table provides a description of the IP Configuration window

Table 15-4 .IP Configuration Window Parameters

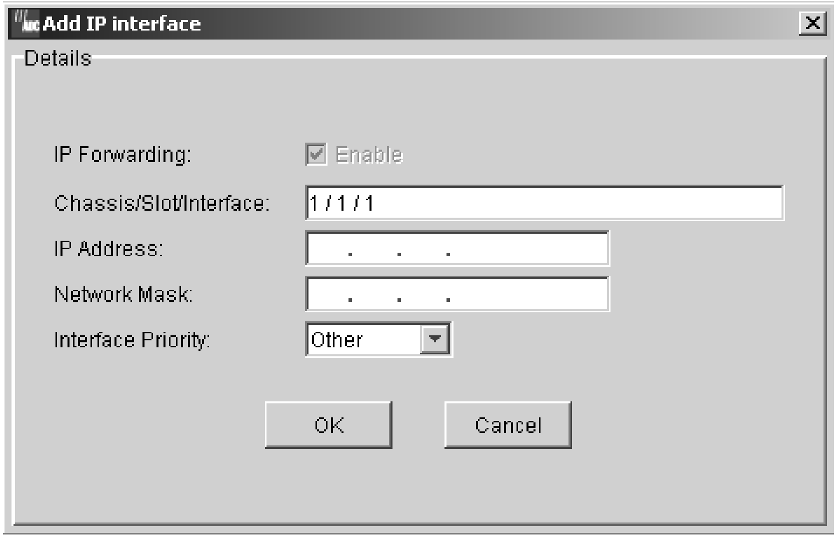
Parameter	Description
Chassis	Number that you assign to the chassis in the network.
Slot	Physical slot in which the interface module is installed.
Interface	Number of the physical interface on the interface module.
Class	Indicates that the interface is Egress.
Type	Indicates the interface type. The Cuda 12000 supports the these types:
CMTS	Includes the docsCableMAClayer MIB object.
Ethernet	Includes the 10 Mb, 100 Mb, or Gigabit interfaces.
POS	Includes the OC-3 and OC-12 interfaces.

Parameter	Description
Status	Indicates whether the interface is up (in service) or down (not in service).
IP Addr	IP address for this interface
Net Mask	Network mask for this interface.
Interface Priority	Specifies the priority of the source IP address for sending packets originating at the interface.
Reasm Size	Largest IP datagram that the router can reassemble from incoming IP fragmented datagrams received on the interface.

5. Click **Add**. The Add IP Interface window appears (Figure 12-5, "Add IP Interface Window").
6. Enter the IP Address, Network Mask, and Priority that you want to use for the bridge group. Refer to Table 15-5.
7. Click **Ok** to commit the entry or **Cancel** to exit without saving.

What You See

Figure 15-5 Add IP Interface Window



Add IP interface

Details

IP Forwarding: ☑ Enable

Chassis/Slot/Interface: 1 / 1 / 1

IP Address: . . .

Network Mask: . . .

Interface Priority: Other

Parameter Descriptions

This table provides a description of the Add IP Interface window

Table 15-5 Add IP Interface Window Parameters.

Parameter	Description
IP Forwarding	By default, IP Forwarding is Enabled for the interface.
Chassis/Slot/Interface	Indicates the chassis, slot, and interface for which you wish to add an IP interface.
IP Address	Source IP address for packets originating at the interface.
Network Mask	Network mask for this interface.

Parameter	Description
Interface Priority	Specifies the priority of the source IP address for sending packets originating at the interface. Select the preference for this IP address relative to other IP addresses on the interface. The options are: Primary, Secondary, or Other. For example, if you wish the source IP address for ICMP redirect to use this IP address, select Primary. If you wish to use a different IP address, then select Secondary. If you do not have a preference, select Other.

The address that you assign to the bridge group is automatically added to the routing table.

Assigning Bridged Interfaces to Gateways

Gateway Addresses are used by the DHCP Relay to request a specific IP address for the host, cable modem, and MTA devices. *Keep in mind that, for DHCP Relay purposes, Host refers to CPE and IP LAN Host.*

For more information about DHCP Relay, and Gateway Addresses, refer to Chapter 16, "Configuring DHCP Relay".

To assign bridged interfaces to host, cable modem and MTA gateways, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **IP** > **DHCP**.
2. In the DHCP Summary window, select the row that includes the bridged interface to which you want to assign a gateway address.
3. Click the **DHCP Relay** tab.
4. Click the **DHCP Relay Options** tab. Enable the DHCP Relay Enabled and DHCP Agent Options by selecting the option.
5. To assign a host, CM or MTA gateway for the selected interface, choose the following options:

a To assign a host gateway, from the Gateway Summary window select the gateway address that you want to assign to the host. Go to the Host Gateway Address field and choose **Set Gateway**.

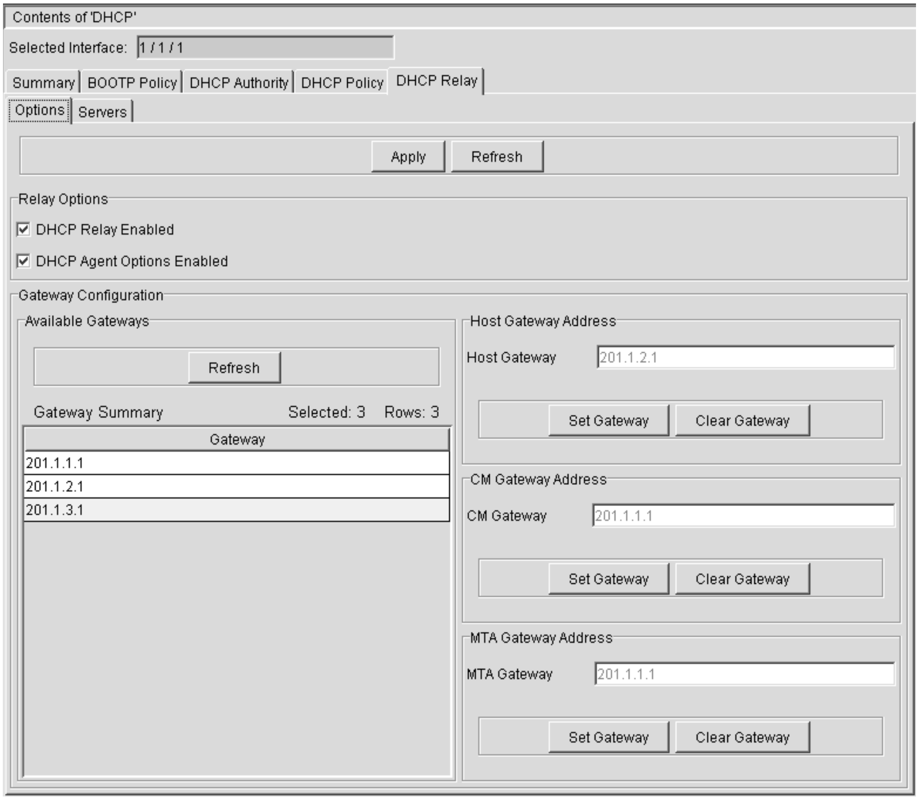
b To assign a CM gateway, from the Gateway Summary window select the gateway address that you want to assign to the cable modem. Go to the CM Gateway Address field and choose **Set Gateway**.

c To assign a MTA gateway, from the Gateway Summary window select the gateway address that you want to assign to the cable modem. Go to the MTA Gateway Address field and choose **Set Gateway**.

What You See

This figure shows an example of the DHCP Relay Options window.

Figure 15-6 DHCP Relay Options Window



Contents of 'DHCP'

Selected Interface: 1 / 1 / 1

Relay Options

☑ DHCP Relay Enabled

☑ DHCP Agent Options Enabled

Gateway Configuration

Available Gateways

Gateway Summary Selected: 3 Rows: 3

Gateway
201.1.1.1
201.1.2.1
201.1.3.1

Host Gateway Address

Host Gateway: 201.1.2.1

CM Gateway Address

CM Gateway: 201.1.1.1

MTA Gateway Address

MTA Gateway: 201.1.1.1

Parameter Descriptions

This table describes the parameters of the DHCP Relay Options Window

Table 15-6 DHCP Relay Options Window Parameters.

Parameter	Description
DHCP Relay Enabled	Choose Enable if you want to use DHCP relay on the selected interface. Disable prevents hosts on this interface from being assigned addresses by the DHCP server.

Parameter	**Description**
DHCP Agent Option Enabled	Choose Enable if you configure your provisioning servers to authenticate cable modems, CPE devices and MTA devices.
Gateway Summary	The current list of IP addresses on the selected interface.
Host Gateway Address	The gateway IP address to assign to the CPE or IP LAN host.
CM Gateway Address	The gateway IP address to assign to the cable modem host.
MTA Gateway Address	The gateway IP address to assign to the MTA device host.

Setting Bridge Flow Timers

You can configure time-out values for:

- The time that the bridge waits before the bridge entry is removed from the bridge table
- The time before attempting to time-out flows that are not active or the destination of the flow is not reachable.

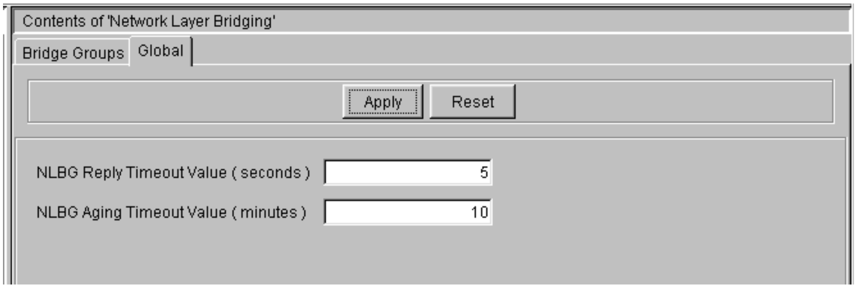
To set the time out values for bridging, follow this procedure:

Before You Begin

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **IP** > **Network Layer Bridging**.

1. Click the **Global** tab.
2. Enter values for these parameters:
3. Click **Apply** to commit the changes or click **Reset** to return to the default values.

Figure 15-7 Bridging Global Window



NLBG Reply Timeout Value (seconds) 5
NLBG Aging Timeout Value (minutes) 10

Parameter Descriptions

This table describes the parameters of the Global window.

Table 15-7 Bridging Global Parameters

Parameter	Description
NLBG Reply Timeout Value (in seconds)	The time, in seconds, to wait for a response for a broadcast flow request before the bridge entry is removed. The default is 2 seconds.

Parameter	Description
NLBG Aging Timeout Value (in minutes)	The time, in minutes, to wait before the aging of entries in the table start. The default is 10 minutes.

16 CONFIGURING DHCP RELAY

This chapter provides information and procedures on how to configure DHCP relay on a cable interface and includes the following sections:

- About DHCP Relay
- Configuring DHCP Relay Options
- Configuring the DHCP Server
- Configuring DHCP Authority
- Configuring DHCP Policies
- Defining BOOTP Polices

About DHCP Relay

DHCP is used within a DOCSIS- or EuroDOCSIS-compliant network to allocate IP addresses and to configure cable modems with other IP parameters.

DHCP Relay support on DOCSIS or EuroDOCSIS modules enables a cable interface (CMTS) to forward DHCP Requests from cable modems, CPE devices, MTA devices, and other IP hosts to a DHCP server. The DHCP server may reside:

- Externally, on a system other than the Cuda 12000 that has the cable interface you are configuring.
- Internally, on the same Cuda 12000 that has the cable interface that you are configuring.

Note: You may configure the CMTS to forward DHCP Requests to up to 32 servers using DHCP Policies. For more information, see "DHCP and BOOTP Policies" on page 449.

Gateway addresses are used by the DHCP Relay to request a specific subnet for the host and cable modem. Configuring DHCP Relay involves:

- Enabling or disabling DHCP Relay
- Configuring the following gateway addresses:
  - **CPE/IP Host Gateway Address** — The Host Gateway address that the DHCP Relay requests on behalf of the host. This is the same address as the Gateway Address configured on the interface. When a DHCP request is received and it is from the host, then the Host Gateway Address is used by the DHCP Relay.
  - **Cable Modem (CM) Gateway Address** — The CM Gateway address that the DHCP Relay requests on behalf of the cable modem. This is the same address as the Gateway Address configured on the interface. When a DHCP Request is received and it is from the cable modem, then the CM Gateway Address is used by the DHCP Relay.
  - **MTA Gateway Address** — The MTA Gateway address that the DHCP Relay requests on behalf of the MTA device. This is the same address as the Gateway Address configured on the interface.When a DHCP

Request is received and it is from the MTA device, then the MTA Gateway Address is used by the DHCP Relay.

- Enabling or disabling agent options.

Refer to RFC3046 for a description of DHCP Relay options.

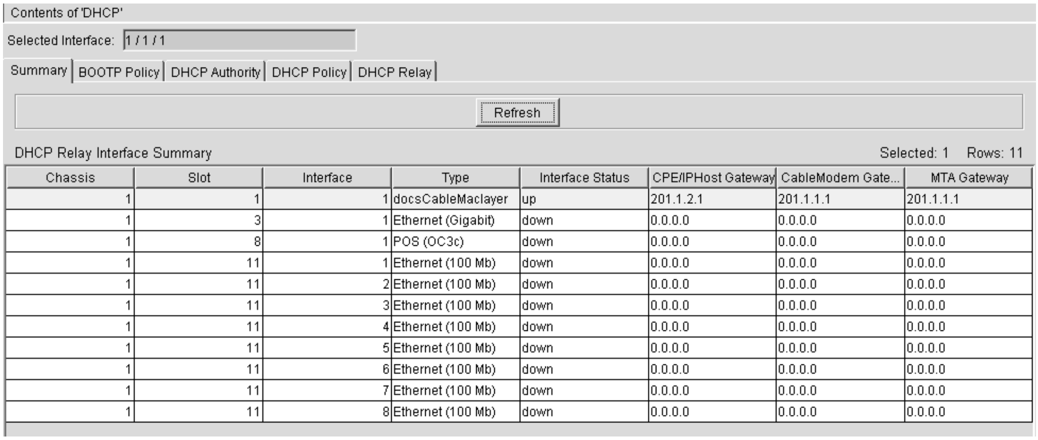
Before You Begin

Before you begin to configure DHCP Relay, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **IP** > **DHCP.**
2. Click the **Summary** tab.
3. Click **Refresh** to update the information.

What You See

Figure 16-1 DHCP Summary Window



Selected Interface: 1 / 1 / 1

DHCP Relay Interface Summary Selected: 1 Rows: 11

Chassis	Slot	Interface	Type	Interface Status	CPE/IPHost Gateway	CableModem Gate...	MTA Gateway
1	1	1	docsCableMaclayer	up	201.1.2.1	201.1.1.1	201.1.1.1
1	3	1	Ethernet (Gigabit)	down	0.0.0.0	0.0.0.0	0.0.0.0
1	8	1	POS (OC3c)	down	0.0.0.0	0.0.0.0	0.0.0.0
1	11	1	Ethernet (100 Mb)	down	0.0.0.0	0.0.0.0	0.0.0.0
1	11	2	Ethernet (100 Mb)	down	0.0.0.0	0.0.0.0	0.0.0.0
1	11	3	Ethernet (100 Mb)	down	0.0.0.0	0.0.0.0	0.0.0.0
1	11	4	Ethernet (100 Mb)	down	0.0.0.0	0.0.0.0	0.0.0.0
1	11	5	Ethernet (100 Mb)	down	0.0.0.0	0.0.0.0	0.0.0.0
1	11	6	Ethernet (100 Mb)	down	0.0.0.0	0.0.0.0	0.0.0.0
1	11	7	Ethernet (100 Mb)	down	0.0.0.0	0.0.0.0	0.0.0.0
1	11	8	Ethernet (100 Mb)	down	0.0.0.0	0.0.0.0	0.0.0.0

Parameter Descriptions

This table provides a description of the DHCP Summary window

Table 16-1 DHCP Summary Parameters.

Parameter	Description
Chassis	Indicates the number identifying the chassis in the network.

Parameter	Description
Slot	Indicates the physical slot in which the module is installed. Chassis slots are numbered from left to right.
Interface	Indicates the number of the interface on the module itself.
Type	Indicates whether the type of interface is CMTS, (docsCableMaclayer), Ethernet (10 Mb, 100 Mb or Gigabit) or POS (OC-3c or OC-12c).
Interface Status	Indicates the operational status of the module. The options are: Up or Down.
CPE/IP Host Gateway	One of the gateway addresses configured on the interface. It is the address that the DHCP Relay discovers on behalf of the requesting CPE/IP Host device.
Cable Modem Gateway	One of the gateway addresses configured on the interface. It is the address that the DHCP Relay discovers on behalf of the cable modem.
MTA Gateway	One of the gateway addresses configured on the interface. It is the address that the DHCP Relay discovers on behalf of the MTA.

Configuring DHCP Relay Options

The purpose of DHCP Relay Options is to enable DHCP Relay and DHCP Agent Options, and to set the Gateway Interface Addresses.

- DHCP Relay Enabled determines if the DHCP Relay is forwarding requests to the DHCP Server.
- DHCP Agent Options Enabled determines if the DHCP Agent Options are added to the request.

The DHCP assigns IP addresses to cable modems. MTAs, and hosts; the addresses must be in the range of IP addresses represented by the Gateway Interface Address.

- The Host Gateway Address must be set in order for the DHCP server to perform the assignment.
- The Host *and* CM Gateway Addresses must be set if the interface is a CMTS.

Agent (Option 82) adds the cable modem MAC address, the MTA MAC address, and the Interface that issued the DHCP request.

To configure DHCP relay options follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **IP** > **DHCP.**
2. Click the **Summary** tab.
3. In the Summary window, select the row that includes the interface that you want to configure.
4. Click the **DHCP Relay** tab. The Relay Options window appears. Refer to Figure 16-2.
5. In the Relay Options section, enter parameter values. Refer to Table 16-1.
6. Click Refresh to update the information.
7. Go to the **Gateway Configuration** section to select an IP address to use as the Host Gateway, the CM Gateway and the MTA Gateway. The Gateway is on the subnet from which the DHCP server assigns IP addresses to the cable modems and/or hosts. Choose the following options:

8. To assign the gateway for the CPE and IP LAN hosts, select the IP address from the Gateway Summary list. Go to the **Host Gateway Address** section and click **Set Gateway**. This automatically adds the address to the Host Gateway field. The Host Gateway picks the subnet that the DHCP relay requests from the DHCP server for the host.

9. To assign the gateway for the cable modem hosts, select the IP address from the Gateway Summary list. Go to the **CM Gateway Address** section and click **Set Gateway**. This automatically adds the address to the CM Gateway field. The CM Gateway is used to pick the subnet that the DHCP relay requests from the DHCP server for a cable modem.

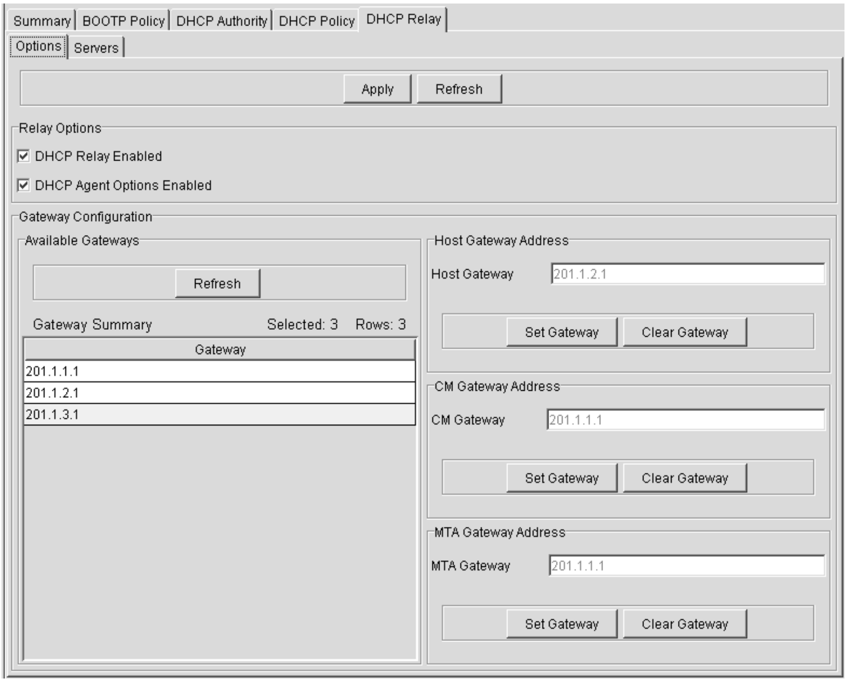
10. To assign the gateway for the MTA device hosts, select the IP address from the Gateway Summary list. Go to the **MTA Gateway Address** section and click **Set Gateway**. This automatically adds the address to the MTA Gateway field. The CM Gateway is used to pick the subnet that the DHCP relay requests from the DHCP server for a cable modem.

11. To clear a gateway address, go to the gateway address that you want to clear and choose **Clear Gateway.**

12. After you complete configuration, choose **Apply** to save the configuration.

What You See

Figure 16-2 DHCP Relay Options Window



☑ DHCP Relay Enabled

☑ DHCP Agent Options Enabled

Gateway Summary Selected: 3 Rows: 3

Gateway
201.1.1.1
201.1.2.1
201.1.3.1

Host Gateway: 201.1.2.1

CM Gateway: 201.1.1.1

MTA Gateway: 201.1.1.1

Parameter Descriptions

This table descirbes the parameters in the Relay Options window.

Table 16-1 Relay Options Window Parameters

Parameter	Description
DHCP Relay Enabled	Choose Enable if you want to use DHCP relay on this interface. Disable prevents hosts on the interface from being assigned addresses by the DHCP server.
DHCP Agent Option Enabled	Choose Enable if you configure your provisioning servers to authenticate cable modems, and CPE devices.

Configuring the DHCP Server

The purpose of DHCP Server configuration is to add a DHCP Server, to which DHCP Relay requests are forwarded. DHCP Servers are assigned on a per interface basis.

If a DHCP server is not configured, then the DHCP relay drops all DHCP requests as it does not know where to forward them.

Adding DHCP Servers

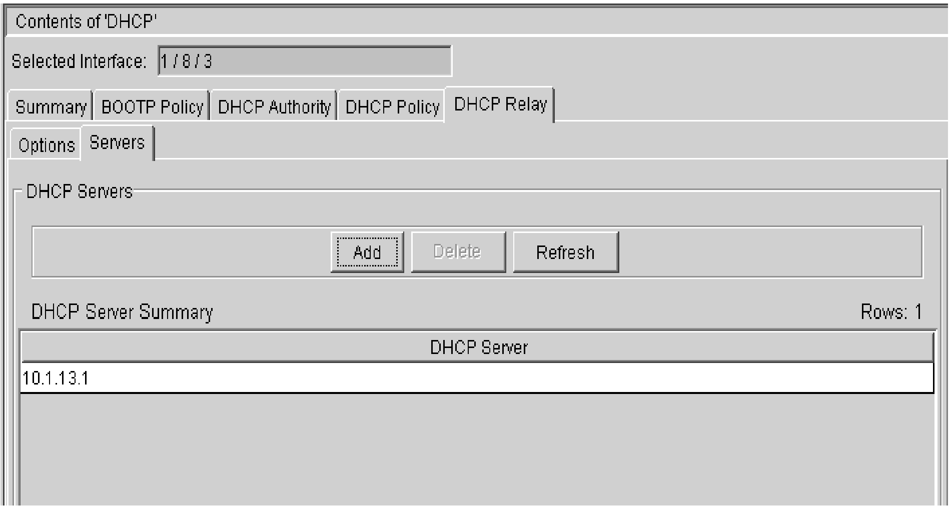
To add a DHCP Server follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **IP** > **DHCP.**
2. Click the **Summary** tab.
3. Click **Refresh** to update the information.
4. In the Summary window (Figure 16-1), select the row that includes the interface to which you want to add a DHCP Server.
5. Click the **DHCP Relay** tab.
6. Click the **Servers** tab. The Servers window appears and displays DHCP Servers already assigned to that interface. For example, if the display is empty it means that there are no DHCP Servers assigned to that interface.
7. Click **Add.** The Add DHCP Server Host window appears.
8. Enter the DHCP Server IP address to be used for the selected interface.
9. Click **Ok** to commit the information or click **Cancel**.

What You See

This figure shows an example of the Servers window.

Figure 16-3 DHCP Servers Window



Selected Interface: 1 / 8 / 3

Rows: 1

DHCP Server
10.1.13.1

Deleting DHCP Server

To remove a DHCP Server from an interface follow these steps:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **IP** > **DHCP.**
2. Click the **Summary** tab.
3. Click **Refresh** to update the information.
4. In the Summary window, select the row that includes the interface from which to remove the DHCP Server.
5. Click the **DHCP Relay** tab.
6. Click the **Servers** tab.
7. Select the DHCP server that you want to delete.
8. Choose **Delete.** A confirmation window appears.
9. Click **Yes** to continue or click **No** to exit cancel.

Configuring DHCP Authority

DHCP authority is a security feature that prevents spoofing *(unauthorized use)* of DHCP assigned IP addresses. Spoofing occurs when a host uses an IP address that was dynamically assigned to another host via DHCP. DHCP Authority prevents spoofing of IP addresses by ensuring that IP addresses are only used by the specific cable modems and the CPE devices to which they are assigned.

Configured on an interface basis, DHCP Authority ensures that dynamically assigned IP addresses are used by their original host by tagging Address Resolution Protocol (ARP) entries within the ARP cache for a specified interface.

This DHCP Authority ARP entry tagging process operates as follows:

- Upon booting, the client (such as a cable modem or CPE device) requests an IP address from the DHCP server. The DHCP relay agent operating on the interface to which the client is attached, forwards the request to the DHCP server.
- Based on the subnet configuration within the provisioning server, the DHCP server responds with a DHCP offer containing the IP address that the client should use.
- After receiving the IP address, the client sends a DHCP Request back to the DHCP server.
- The DHCP server sends an acknowledgement (ACK) to the client through the DHCP relay.
- When the DHCP relay agent sees this acknowledgement, it verifies whether the IP address falls within a DHCP Authority range configured on the interface, and one of these actions occur:
  - If the address does fall within a preconfigured DHCP Authority range and DHCP Authority is enabled for that interface, an ARP entry is added to the ARP cache for that interface and tagged as being assigned via DHCP. This tag is shown as type "`Other`" when viewing the ARP cache for that interface and ensures that specific IP address only maps to that specific MAC address.

    or

- If there is no DHCP Authority range, the entry is simply added to the ARP cache and labelled as type "`Dynamic`" when the ARP mapping is learned.

This feature is termed DHCP Authority because those tagged as being assigned via DHCP take precedence over dynamically assigned *(non-DHCP tagged)* ARP entries.

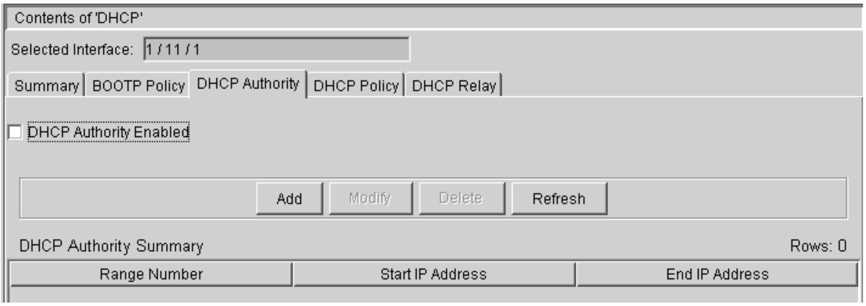
Enabling and Disabling DHCP Authority

To enable or disable DHCP authority on an interface, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **IP** > **DHCP.**
2. Click the **Summary** tab.
3. Click **Refresh** to update the information.
4. In the Summary window, select the row that includes the interface that you wish to enable or disable DHCP authority.
5. Click the **DHCP Authority** tab.
6. Clear or select the DHCP Authority Enabled check box. Selecting the check box enables DHCP Authority. Clearing the check box disables DHCP Authority.

What You See

Figure 16-4 DHCP Authority window.



Contents of 'DHCP'

Selected Interface: 1 / 11 / 1

□ DHCP Authority Enabled

DHCP Authority Summary Rows: 0

Range Number	Start IP Address	End IP Address

Configuring DHCP Authority Ranges

The DHCP Authority ranges that you define for an interface dictate what addresses are protected by the authority feature. The DHCP Authority IP address ranges that you define must fall within the range of IP addresses as allowed by the IP interface *(as dictated by the network mask for that IP interface)*.

For example, if the physical interface has an IP interface of 172.16.19.1with a mask of *255.255.255.0* installed, you can define a DHCP Authority range from *172.16.19.2* to *172.16.19.254*, or any subset of that IP address range. You can define up to 200 IP address ranges per physical interface.

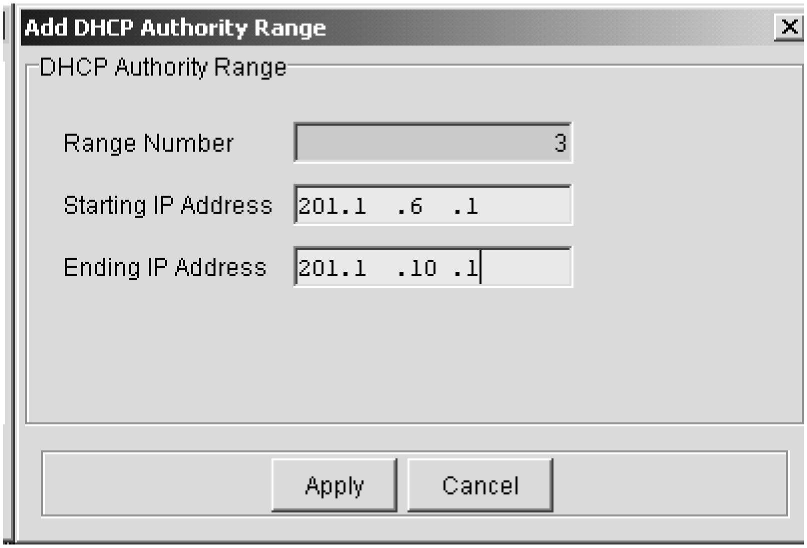
The DHCP Authority ranges take effect upon the next DHCP server exchange with the client. This means that after you configure a range, you should reboot the client so that the ARP entry for that client's MAC address is updated.

To configure DHCP Authority ranges, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **IP** > **DHCP.**
2. Click the **Summary** tab.
3. In the Summary window, select the row that includes the interface on which you want to configure DHCP Authority.
4. Click the **DHCP Authority** tab.

5. Click the **Add** button. The Add DHCP Authority Range window appears.
6. Enter values for these parameters:
   - Starting IP Address — Starting IP address for the DHCP Authority range.
   - Ending IP Address — Ending IP address for the DHCP Authority range.
7. Click **Apply** to save the entries or click **Cancel** to exit without saving.

Figure 16-5 Add DHCP Authority Range Window



Add DHCP Authority Range

DHCP Authority Range

Range Number: 3

Starting IP Address: 201.1 .6 .1

Ending IP Address: 201.1 .10 .1

Modifying DHCP Authority Ranges

To modify DHCP Authority ranges, follow this procedure:

1. In the Summary window, select the row that includes the interface on which you want to configure DHCP Authority.
2. Click the **DHCP Authority** tab.
3. Click **Modify**.
4. Enter changes to the information.
5. Click **Apply** to save the changes or click **Cancel** to exit without saving.

Deleting DHCP Authority Ranges

To delete DHCP Authority ranges, follow this procedure:

1. From the DHCP Authority window, select the row that includes the range you want to delete.
2. Click **Delete**. A confirmation window appears.
3. Click **Yes** to continue or click **Cancel**.

DHCP and BOOTP Policies

You can use Dynamic Host Configuration Protocol (DHCP) policies to control which devices obtain IP addresses and which servers allocate those addresses.

A DOCSIS-compliant network uses DHCP for dynamic assignment of IP addresses. A DHCP server allocates addresses and other IP operational parameters to requesting cable modems and CPE devices. DOCSIS and EuroDOCSIS modules serve as Cable Modem Termination Systems (CMTS) and, as such, also function as DHCP relay agents. As relay agents, these cable interfaces relay DHCP requests and responses between the DHCP server, cable modems, and CPE devices.

DHCP policies allow you to control and restrict the forwarding of DHCP requests. Specifically, DHCP policies allow matching on several parameters in the DHCP packet. It then uses the result of this matching to determine which list of servers to forward the packet to; or it can reject (drop) the packet to deny the requesting client an address. The relay agent on the CMTS can also forward Bootstrap Protocol (BOOTP) requests. You can create similar policies to control the servers to which the interface forwards BOOTP requests.

DHCP and BOOTP policies allow you to:

- Prevent selected cable modems and CPE devices from obtaining IP addresses.
- Direct DHCP requests to particular DHCP servers based on whether the request originated from a cable modem or CPE device.
- Direct DHCP requests to particular DHCP servers based on the cable modem's or CPE's MAC address.
- Direct DHCP requests to particular servers based on which interface it was received.

For example, you can configure the system to match on the DHCP packet to determine whether the request originated from a cable modem, a CPE, a specific interface, or a specific MAC address; wildcards can be used to match portions of a MAC address. In the event of a match, you can configure the DHCP relay agent to forward the request to a list of up to three DHCP servers, or configure the agent to drop the request.

If there are no policies defined, or a DHCP packet does not match any existing policy, the default policy is used to determine if the packet is dropped or forwarded to a list of up to three DHCP servers. The system ships with a default policy to deny *(drop)* DHCP requests that do not match any other policy. Note that while other DHCP policies are interface-specific, the default DHCP policy is module-wide—it provides default behavior for all interfaces on the module. This default policy can be modified but not deleted.

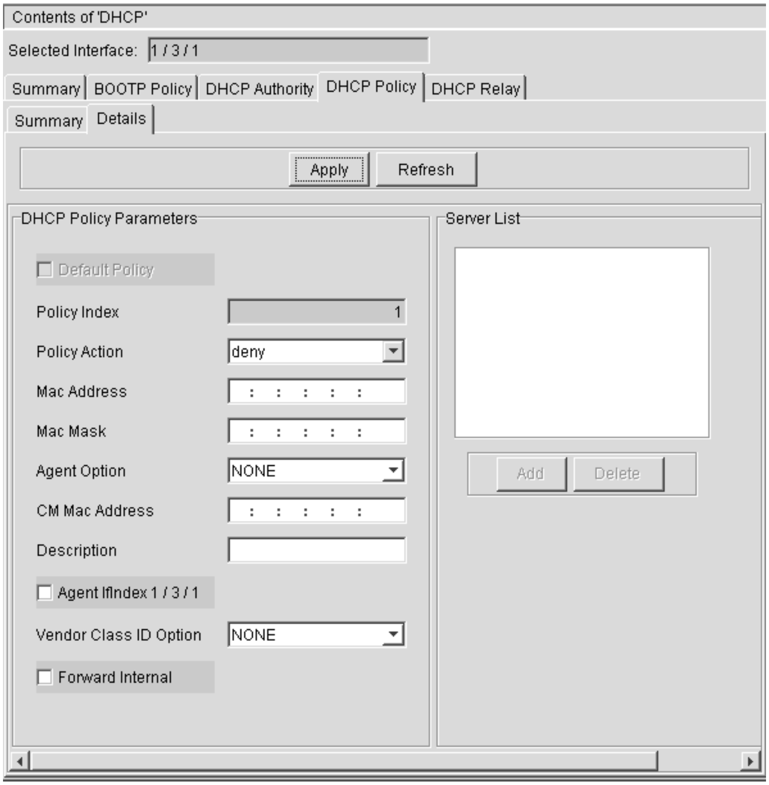
Configuring DHCP Policies

DHCP policies determine the DHCP servers to which a CMTS interface forwards DHCP requests from attached cable modems and CPE devices.

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **IP** > **DHCP.**
2. Click the **Summary** tab.
3. In the DHCP Summary window (Figure 16-1), select the row that includes the interface on which you want to configure DHCP policies.
4. Click the **DHCP Policy** tab.
5. Click the **Add** button. The Details window appears.
6. Enter values for these parameters.
7. Click **Refresh** to update the information.

What You See

Figure 16-6 DHCP Policy Details window



Contents of 'DHCP'

Selected Interface: 1 / 3 / 1

☐ Default Policy

Policy Index: 1

Policy Action: deny

Mac Address: : : : : :

Mac Mask: : : : : :

Agent Option: NONE

CM Mac Address: : : : : :

Description:

☐ Agent IfIndex 1 / 3 / 1

Vendor Class ID Option: NONE

☐ Forward Internal

Parameter Descriptions

This table provides a description of the Details window

Table 16-2 DHCP Policy Details Window.

Parameter	Description
Policy Index	This number determines the sequence in which a DHCP request is compared to each policy. You assign this number when defining the policy. The request is applied to the policy with the lowest index first, then precedes incrementally. Upon finding a match, the action defined for the policy is taken, and no further policies are applied.

Parameter	Description
Policy Action	The action that you want the system to take upon finding a matching DHCP request. You can configure the interface to either permit the packet to be forwarded to up to three DHCP servers or deny (drop) the packet without forwarding.
Mac Address	Allows you to match on the source MAC address of the cable modem. You can also set any or all octets of the MAC address as a wild card.
Mac Mask	Allows you to match on the source MAC mask of the cable modem. You can also set any or all octets of the MAC mask as a wild card.
Agent Option	Determines whether the DHCP request is from a cable modem or CPE device.
CM Mac Address	Allows you to match on the cable modem MAC address contained in the request.
Description	Descriptive term to identify the DHCP policy.
Agent IfIndex	Enables you to match on the specific interface on which the DHCP offer was received.
Forward Internal	Specifies whether the current cable interface forwards DHCP requests internally (meaning, to a DHCP server on the local Cuda 12000). Select this option to enable internal forwarding; or, deselect to disable internal forwarding.

Modifying a DHCP Policy

Modifying a default DHCP policy allows you to permit forwarding for up to three DHCP servers. *Modifying does not allow you to define matching criteria for the default policy.*

To modify a DHCP policy, follow this procedure:

1. Click the **DHCP Policy** tab.
2. Click the **Summary** tab.
3. Select the row that includes the policy that you want to modify.
4. Click the **Modify** button. The Details window appears (Figure 16-6, “DHCP Policy Details window”).
5. Modify the necessary parameters.
6. Click **Apply**.

7. Click **Refresh** to update the information.

Deleting a DHCP Policy

To delete a DHCP Policy, perform this procedure:

You cannot delete the default DHCP policy.

1. Click the **DHCP Policy** tab.
2. Click the **Summary** tab.
3. Select the row that includes the policy that you want to delete.
4. Click the **Delete** button. A confirmation window appears.
5. Click **Yes** to delete the policy or click **No** to exit without deleting the policy.

Defining BOOTP Polices

BOOTP Policies determine the BOOTP servers to which a CMTS interface forwards BOOTP requests from attached cable modems and diskless workstations.

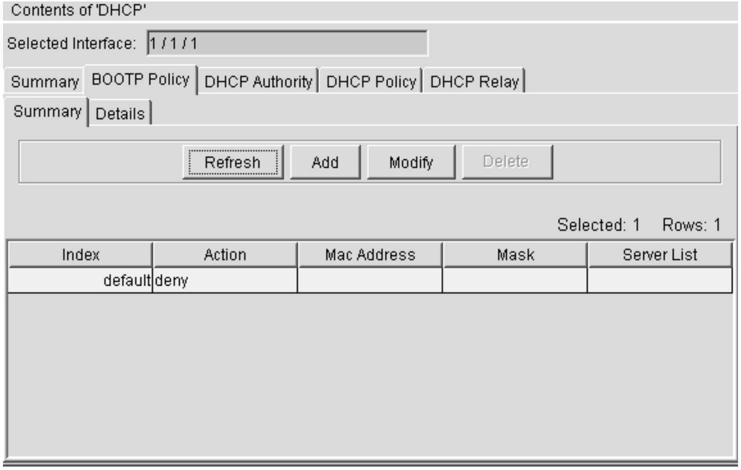
To define BOOTP policies, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **IP** > **DHCP.**
2. Click the **Summary** tab.

1. In the DHCP Summary window (Figure 16-1, “DHCP Relay Options Window”), select the row that includes the interface on which you want to configure BOOTP policies.

1. Click the **BOOTP Policy** tab.
2. Click the **Summary** tab.
3. Click **Add**. The Details window displays. Refer to Figure 16-8.
4. Enter values for these parameters. Refer to Table 16-4.
5. Click **Apply** to commit the information.
6. Click **Refresh** to update the information.

Figure 16-7 BOOTP Policy Summary Window



Contents of 'DHCP'

Selected Interface: 1 / 1 / 1

Selected: 1 Rows: 1

Index	Action	Mac Address	Mask	Server List
default	deny			

Parameters

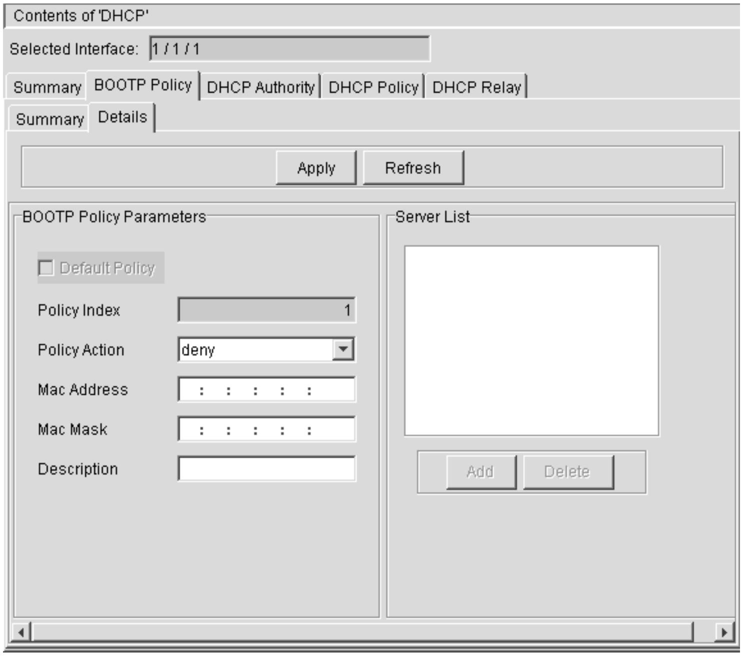
This table summarizes the BOOTP Policy Summary window parameters

Table 16-3 BOOTP Policy Summary Window Parameters.

Parameter	Description
Index	This number determines the sequence in which a BOOTP request is compared to each BOOTP policy. You assign this number when defining the policy. The request is applied to the policy with the lowest index first, then precedes incrementally. Upon finding a match, the action defined for the policy is taken, and no further policies are applied.
Action	The action that you want the system to take upon finding a matching BOOTP request. You can configure the interface to either permit the packet to be forwarded to up to three DHCP servers or deny (drop) the packet without forwarding.
Mac Address	Allows you to match on the source MAC address of the cable modem. You can also set any or all octets of the MAC address as a wild card.
Mac Mask	Allows you to match on the source MAC mask of the cable modem. You can also set any or all octets of the MAC mask as a wild card.
Server List	A list of IP addresses to which you want the current cable interface to forward DHCP packets.

What You See

Figure 16-8 BOOTP Policy Details Window


Contents of 'DHCP'

Selected Interface: 1 / 1 / 1

□ Default Policy

Policy Index: 1

Policy Action: deny

Mac Address: : : : : :

Mac Mask: : : : : :

Description:

Parameter Descriptions

This table provides a description of the Details window

Table 16-4 BOOTP Policy Details Window.

Parameter	Description
Policy Index	This number determines the sequence in which a DHCP request is compared to each policy. You assign this number when defining the policy. The request is applied to the policy with the lowest index first, then precedes incrementally. Upon finding a match, the action defined for the policy is taken, and no further policies are applied.
Policy Action	The action that you want the system to take upon finding a matching DHCP request. You can configure the interface to either permit the packet to be forwarded to up to three DHCP servers or deny (drop) the packet without forwarding.

Parameter	Description
Mac Address	Allows you to match on the source MAC address of the cable modem. You can also set any or all octets of the MAC address as a wild card.
Mac Mask	Allows you to match on the source MAC mask of the cable modem. You can also set any or all octets of the MAC mask as a wild card.
Description	Descriptive term to identify the DHCP policy.

Modifying a BOOTP Policy

Modifying a default BOOTP policy allows you to permit forwarding for up to three DHCP servers. *Modifying does not allow you to define matching criteria for the default policy.*

To modify a BOOTP policy, perform this procedure:

1. Click the **BOOTP Policy** tab.
2. Click the **Summary** tab.
3. Select the row that includes the policy that you want to modify.
4. Click the **Modify** button. The Details window appears (Figure 16-8, “BOOTP Policy Details Window”).
5. Modify the parameters as required.
6. Click **Apply**.

Deleting a BOOTP Policy

To delete a BOOTP Policy, perform this procedure:

You cannot delete the default BOOTP policy.

1. Click the **BOOTP Policy** tab.
2. Click the **Summary** tab.
3. Select the row that includes the policy that you want to modify.
4. Click **Delete**. A confirmation window appears.
5. Click **Yes** to delete the policy or click **No** to cancel.

17 IP MULTICAST

This chapter describes how to manage IP Multicast on the Cuda 12000, and includes the following sections:

- About IP Multicast
- Managing IGMP Interfaces
- Configuring IGMP Groups
- Configuring IGMP Proxy
- Viewing IP Multicast Routes

About IP Multicast

IP Multicast reduces traffic on a network by delivering a single stream of information to multiple users at one time. The Cuda 12000 supports up to 500 multicast groups per chassis.

IGMP

Internet Group Management Protocol (IGMP) is required by all hosts and routers to receive or forward multicast packets.

A host uses IGMP to report its multicast group memberships to directly connected routers. When a host joins a multicast group, it sends an IGMP host membership report message, declaring its membership in a specific group. If the host has multiple interfaces, the host declares its membership in a specific group for each interface on which it joins that group.A host can join multiple multicast groups on a single interface.

When a host receives multicast traffic on an interface on which it has joined a multicast group, it then forwards the traffic to each and every other interface on which it has joined that same multicast group. For example, if on interfaces A, B, and C, a host joins a multicast group, Group1, and receives traffic destined for Group 1 on interface B, it can forward the traffic on the other interfaces A and C.

One instance of IGMP runs on each interface. The IGMP for that interface has no knowledge of any multicast groups on any other interfaces.

A multicast router uses IGMP to determine which multicast groups have members that are directly connected to the router on each of the router’s physical interfaces. It keeps a list of multicast group memberships for each physical interface.

You can configure an IP interface on the Cuda 12000 IP Access Switch to perform one of the following roles:

- IGMP Querier Role — The Cuda 12000 IP Access Switch, through the IP interface thus configured, periodically transmits IGMP queries to determine which multicast groups are directly connected on an interface.

- IGMP Host Role — The Cuda 12000 IP Access Switch, through the IP interface thus configured, receives the queries and replies to the querier with information on each multicast group that needs to receive traffic.

IGMP Proxy

The Cuda 12000 IP Access Switch uses IGMP Proxy to inform a multicast router about members of multicast groups to which the router must forward multicast traffic. These members are directly connected to the Cuda 12000 IP Access Switch on one or more interfaces, but are not directly connected to the multicast router.

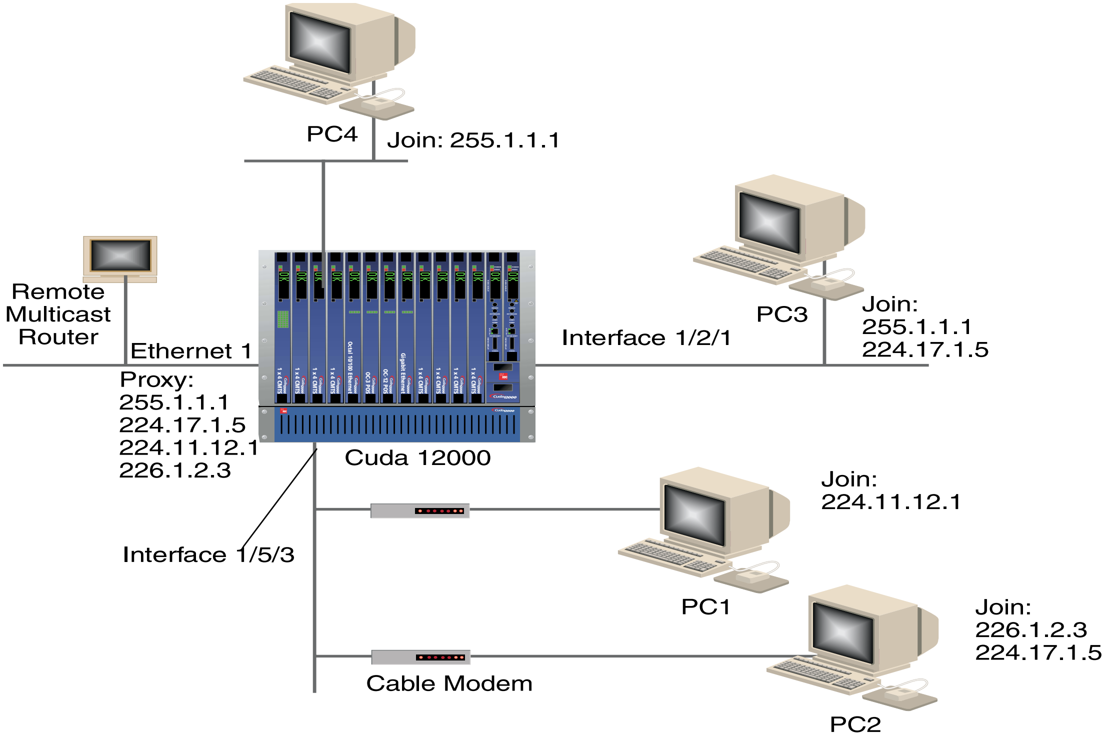
Example

For example, in Figure 17-1, each Cuda 12000 IP interface except the one connected to the remote multicast router is configured to perform the IGMP querier role. The Cuda 12000 sends out IGMP queries on each interface on which it performs the querier role. Each IGMP host that receives these queries replies to the Cuda 12000 with IGMP reports for each multicast group to which the host belongs. The reports tell the Cuda 12000 about the multicast groups to which group members PC4, PC3, PC2, and PC1 belong. To transmit multicast traffic to PC4, PC3, PC2 and PC1, the Cuda 12000 informs the remote multicast router that these multicast group members are requesting to receive traffic for the groups to which they belong.

If IGMP proxy is enabled on the Cuda 12000, the Cuda 12000 joins these multicast groups for the Ethernet interface that connects the Cuda to the remote multicast router (this interface is called the *proxy interface*). When the remote multicast router sends an IGMP query to the Cuda 12000, the Cuda 12000 replies with IGMP reports on behalf of these multicast groups. The remote multicast router can then route multicast traffic destined for these groups onto the Ethernet that connects it to the Cuda 12000, and the Cuda 12000, in turn, can route the multicast traffic to the appropriate destinations.

For example, in the figure, if the remote multicast router receives a multicast packet addressed to 224.17.1.5, the router forwards the packet to the Cuda 12000 across their common Ethernet connection. The Cuda 12000 then receives the packet and forwards it to interface 1/2/1 and 1/5/3. PC3 and PC2 receive the multicast packet.

Figure 17-1 Example Network



Managing IGMP Interfaces

In the Cuda 12000, you can configure the proxy interface for each individual IP Multicast address or a range of multicast addresses. This enables you to specify a proxy interface for a single multicast group to one interface and another multicast group to a different interface. Or you can proxy the entire multicast range to a specific interface.

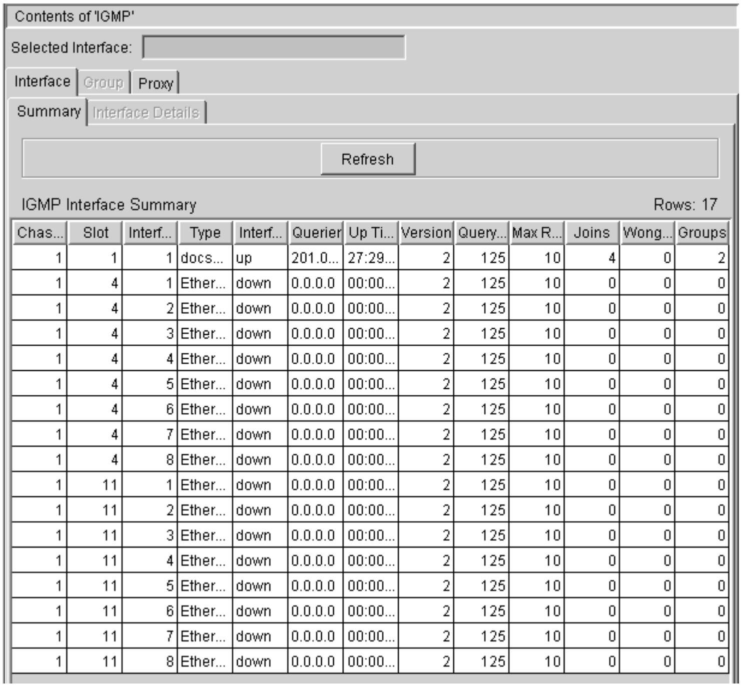
Before You Begin

Before you configure IGMP interfaces, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **IP** > **Multicast** > **IGMP.**
2. Click the **Interface** tab.
3. Click the **Summary** tab. The interface summary table appears.

What You See

Figure 17-2 IGMP Interface Summary Window



IGMP Interface Summary

Rows: 17

Chas...	Slot	Interf...	Type	Interf...	Querier	Up Ti...	Version	Query...	Max R...	Joins	Wong...	Groups
1	1	1	docs...	up	201.0...	27:29...	2	125	10	4	0	2
1	4	1	Ether...	down	0.0.0.0	00:00...	2	125	10	0	0	0
1	4	2	Ether...	down	0.0.0.0	00:00...	2	125	10	0	0	0
1	4	3	Ether...	down	0.0.0.0	00:00...	2	125	10	0	0	0
1	4	4	Ether...	down	0.0.0.0	00:00...	2	125	10	0	0	0
1	4	5	Ether...	down	0.0.0.0	00:00...	2	125	10	0	0	0
1	4	6	Ether...	down	0.0.0.0	00:00...	2	125	10	0	0	0
1	4	7	Ether...	down	0.0.0.0	00:00...	2	125	10	0	0	0
1	4	8	Ether...	down	0.0.0.0	00:00...	2	125	10	0	0	0
1	11	1	Ether...	down	0.0.0.0	00:00...	2	125	10	0	0	0
1	11	2	Ether...	down	0.0.0.0	00:00...	2	125	10	0	0	0
1	11	3	Ether...	down	0.0.0.0	00:00...	2	125	10	0	0	0
1	11	4	Ether...	down	0.0.0.0	00:00...	2	125	10	0	0	0
1	11	5	Ether...	down	0.0.0.0	00:00...	2	125	10	0	0	0
1	11	6	Ether...	down	0.0.0.0	00:00...	2	125	10	0	0	0
1	11	7	Ether...	down	0.0.0.0	00:00...	2	125	10	0	0	0
1	11	8	Ether...	down	0.0.0.0	00:00...	2	125	10	0	0	0

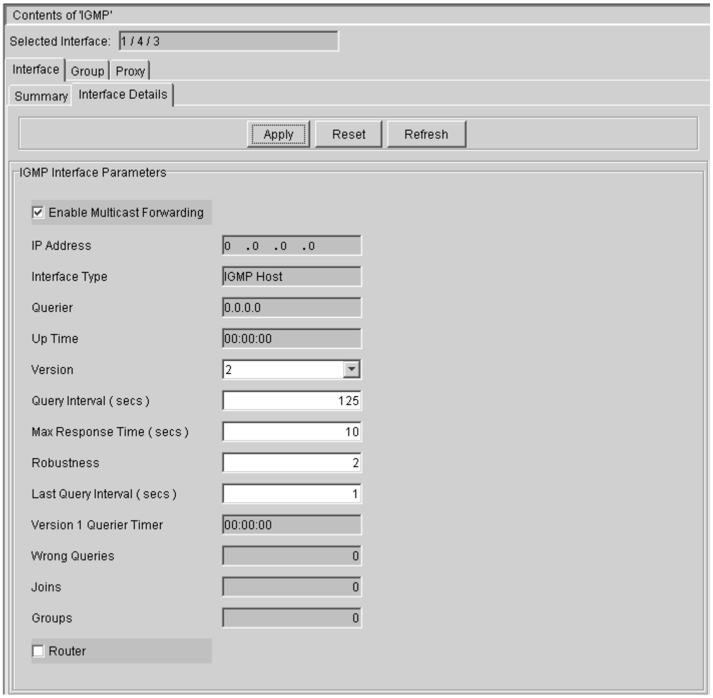
Configuring an IGMP Interface

To configure an IGMP interface, follow these steps:

1. In the **Summary** window, select the interface that you wish to configure.
2. Click the **Interface Details** tab. The Interface Details window appears.
3. Enter values for the parameters. Refer to Table 17-1.
4. Click **Apply** to commit the changes or click **Reset** to change values to default.
5. Click **Refresh** to update the information.

What You See

Figure 17-3 Interface Details window.



Contents of 'IGMP'

Selected Interface: 1 / 4 / 3

IGMP Interface Parameters

☑ Enable Multicast Forwarding

IP Address	0 .0 .0 .0
Interface Type	IGMP Host
Querier	0.0.0.0
Up Time	00:00:00
Version	2
Query Interval (secs)	125
Max Response Time (secs)	10
Robustness	2
Last Query Interval (secs)	1
Version 1 Querier Timer	00:00:00
Wrong Queries	0
Joins	0
Groups	0

☐ Router

Parameter Descriptions

This table provides a description of the Interface Details window.

Table 17-1 Interface Details Window Parameters

Parameter	Description
IP Address	Read-only. The lowest IP address configured on the specified interface. This address uses the same source address of all IGMP packets sent from this interface.
Interface Type	Read-only. Indicates how IGMP is functioning on this interface. The options are:
IGMP Host	Receives IGMP queries and replies for each multicast group for which it wishes to receive traffic.
IGMP Querier	Periodically transmits IGMP queries to finds multicast groups on a network.

Table 17-1 Interface Details Window Parameters (continued)

Parameter	Description
Non-querier	If the current IGMP querier stops functioning, the non-querier interface becomes the querier.
Querier	Read-only. IP address of the IGMP querier on the IP subnet to which this interface is attached.
Up Time	Read-only. Time since the IP address of the IGMP querier changed.
Version	Version of IGMP running on this particular interface. For IGMP to function properly, all routers on a network must be configured to run the same version of IGMP. The default is 2 and the possible values are:
2	Version 2. If the Cuda 12000 encounters another host or router on the network using Version 1, the Cuda 12000 reverts back to using Version 1.
1	Version 1
V2_ONLY	Version 2 only. If the Cuda 12000 encounters another host or router on the network using Version 1, the Cuda 12000 continues to run Version 2.
Query Interval (secs)	Frequency, in seconds, that the IGMP host query packets are transmitted on this particular interface. The default is 125 seconds with a range of 10 to 65535 seconds.
Max Response Time (secs)	Maximum time to wait for a response to an IGMP Query message before the group is deleted. The default is 10 seconds with a range of 1 to 25.
Robustness	Allows you to compensate for the expected packet loss on a subnet. If the loss is expected to be high, increase the value. The default is 2 and the range is 1 to 255.
Last Query Interval (secs)	A query is sent to determine if other hosts on the network wish to receive traffic from the multicast group. The Last Query Interval is the time between queries. You can tune this parameter to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group. The parameter is ignored for Version 1 of IGMP. The default is 1 and the range is 1 to 25 seconds.
Version 1 Querier Timer	Read-only. Remaining time until the Cuda 12000 determines that no IGMPv1 routers are present on the interface. When the value is greater than 0, the host replies to all queries with V1 membership reports.

Table 17-1 Interface Details Window Parameters (continued)

Parameter	**Description**
Wrong Queries	Read-only. Number of queries received indicating that the IGMP version does not match the Version value configured on this interface. IGMP requires all routers on a network to be configured to operate with the same version of IGMP. If any queries indicate the wrong version, this indicates a configuration error.
Joins	Read-only. Number of multicast groups joined on this interface since it was enabled. This parameter reflects the amount of IGMP activity.
Groups	Read-only. Number of current IGMP Groups joined on this interface.
Router	Enables the router to function as either an IGMP Querier (router) or as an IGMP Host. Select the check box to enable the router as an IGMP Querier or clear the check box for the interface to function as an IGMP Host. For the DOCSIS module, the default is router. If multiple routers attempt to become the IGMP querier, the one with the lowest IP address becomes the querier. When you change an interface from a querier to a host, any multicast groups that are learned are removed and any multicast groups joined locally or by an application running on the Cuda 12000 remain. When you change the interface from a host to a querier, any multicast groups joined locally or by an application running on the Cuda 12000 remain. **Note**: The DOCSIS module can only be configured as an IGMP querier (router).

Configuring IGMP Groups

For each interface, you can view, add, or delete an IGMP group. Follow the procedures in this section to configure IGMP groups.

Before You Begin

Before you configure IGMP groups, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **IP** > **Multicast** > **IGMP.**
2. Click the **Interface** tab.
3. Click the **Summary** tab. The interface summary table appears.
4. Click **Refresh** to update the window.

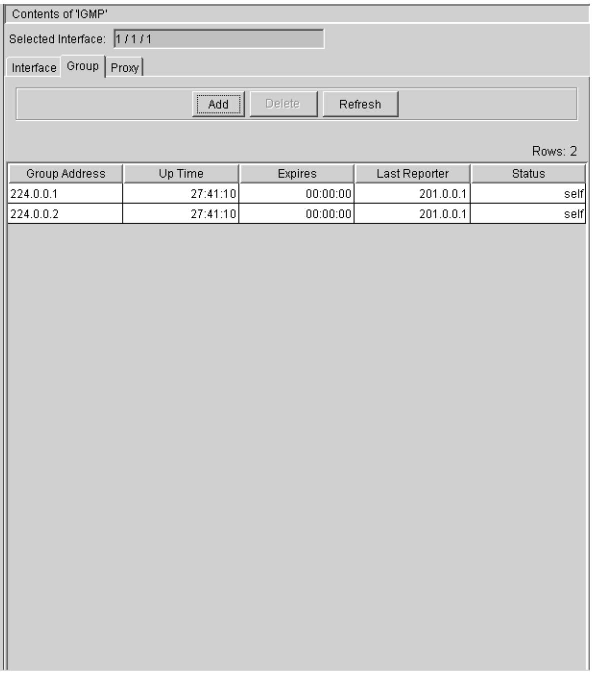
Viewing IGMP Groups

To view IGMP groups for each interface, follow this procedure:

1. In the **Summary** window, select the interface you wish to view.
2. Click the **Group** tab. The Group window appears.
3. Click **Refresh** to update the information.

What You See

Figure 17-4 IGMP Group window.



Selected Interface: 1 / 1 / 1

Rows: 2

Group Address	Up Time	Expires	Last Reporter	Status
224.0.0.1	27:41:10	00:00:00	201.0.0.1	self
224.0.0.2	27:41:10	00:00:00	201.0.0.1	self

Parameter Description

This table provides a description of the IGMP Group window parameters:

Table 17-2 Group Window Parameters

Parameter	Description
Group Address	The IP address of the IGMP group.
Up Time	Time elapsed in hours, minutes, and seconds since the creation of the entry.
Expires	Minimum amount of time remaining before this entry is aged out. If the value is zero, the entry does not time out.
Last Reporter	Source IP address for the last membership report received for this group IP address. If no report is received, the value is 0.0.0.0.
Status	Status of the entry including:
Learned	Group is learned by receiving an IGMP report over the network
Self	Group is locally joined or joined from an application, for example, RIP or OSPF.
Proxy	Group is being proxied on this interface.

Adding IGMP Groups

You can add an IGMP group manually or the group can be learned by receiving IGMP reports over the network. There are no predefined multicast groups.

To add an IGMP group, follow these steps:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **IP** > **Multicast** > **IGMP.**
2. Click the **Interface** tab.
3. Click the **Summary** tab.
4. In the Summary window, select the interface for which you want to add an IGMP group and click the **Group** tab. The Group window appears.
5. Click **Add**. The Add IGMP Group window appears.

6. Enter the group IP address of the IGMP group. The IP address must be within the valid multicast range. If you enter an invalid range, an error message appears.
7. Exit the window by clicking one of these options:
   - **OK** — Commits the changes and returns to the Group window.
   - **Apply** — Commits the changes.
   - **Cancel** — Exits the window without saving.
8. Click **Refresh** to update the information.

Deleting IGMP Groups

To delete an IGMP group from an interface, follow these steps:

You can only delete IGMP groups that you have added through the CLI. Refer to the Cuda 12000 CLI Administration Guide.

1. In the **Summary** window, select the interface that includes the IGMP group you wish to delete.
2. Click the **Group** tab. The Group window appears.
3. Select the group you wish to delete.
4. Click **Delete**. A confirmation window appears.
5. Click **Ok** to commit or **Cancel** to return to cancel the deletion.

Configuring IGMP Proxy

You can configure an interface to proxy for a single multicast group or a range of multicast groups. For each interface, you can also view and delete IGMP proxies.

Before You Begin

Before you configure IGMP proxy, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **IP** > **Multicast** > **IGMP.**
2. Click the **Interface** tab.
3. Click the **Summary** tab. The interface summary table appears.
4. Click **Refresh** to update the window.

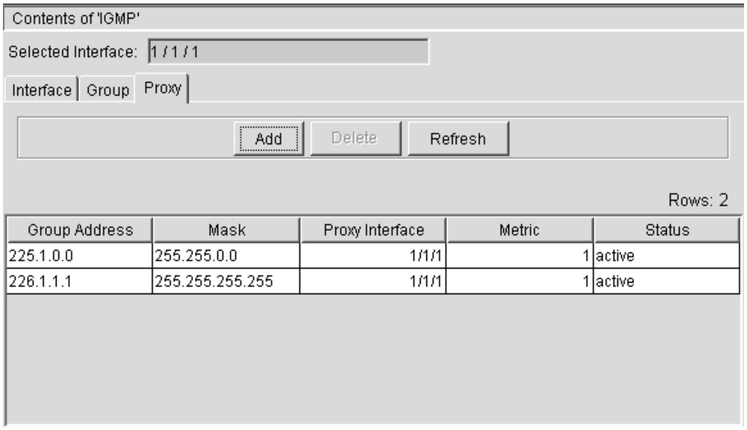
Viewing IGMP Proxies

To view IGMP proxies, follow this procedure:

1. In the **Summary** tab, select the interface that includes the IGMP proxy you with to view.
2. Click the **Proxy** tab. The Proxy window appears.
3. Click **Refresh** to update the information.

What You See

Figure 17-5 IGMP Proxy window.



Contents of 'IGMP'

Selected Interface: 1 / 1 / 1

Rows: 2

Group Address	Mask	Proxy Interface	Metric	Status
225.1.0.0	255.255.0.0	1/1/1	1	active
226.1.1.1	255.255.255.255	1/1/1	1	active

Parameter Descriptions

This table provides a description of the Proxy window.

Table 17-3 Proxy Window Parameters

Parameter	Description
Group Address	Multicast group being proxied.
Mask	Mask applied to the multicast group. A 32 bit IP address specifies one multicast group. A mask of 224.0.0.0 specifies all multicast groups.
Proxy Interface	Interface that proxies for the multicast traffic.
Metric	Metric assigned to this proxy, indicating the priority for the proxy entry.
Status	Status of the proxy.
active	Indicates the proxy is currently in use.
backup	Indicates the proxy is not in use.

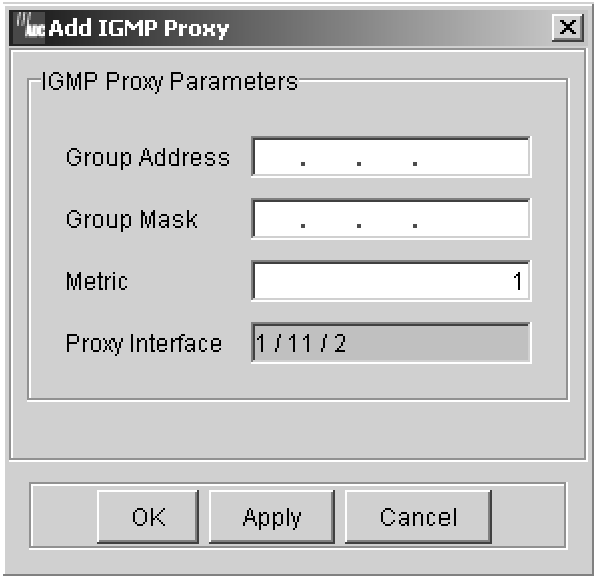
Adding IGMP Proxy

Before adding an IGMP proxy to an interface, you must assign an IP address to that interface. You cannot configure an IGMP proxy for a multicast group within the well known multicast range 224.0.0.0 to 224.0.0.255. If multiple proxies are configured for an interface, the most specific match is used as the proxy for that multicast group. However, if the same ranges are used for the proxies, the metric value determines which proxy is used.

To add an IGMP proxy, follow these steps:

1. In the **Summary** window, select the interface for which you want to add an IGMP proxy.
2. Click the **Proxy** tab. The Proxy window appears.
3. Click **Add**. The Add IGMP Proxy window Appears.
4. Enter values for the parameters. Refer to Table 17-4.
5. Exit the window by clicking one of these options:
   - **OK** — Commits the changes and returns to the Group window.
   - **Apply** — Commits the changes.
   - **Cancel** — Exits the window without committing the changes.
6. Click **Refresh** to update the window.

Figure 17-6 Add IGMP Proxy Window



Group Address . . .
Group Mask . . .
Metric 1
Proxy Interface 1 / 11 / 2

Parameter Descriptions

This table provides a description of the Add IGMP Proxy window.

Table 17-4 Add IGMP Proxy Window Parameters

Parameter	Description
Group Address	IGMP group IP address that applies to the proxy.
Group Mask	IGMP group mask ANDed with the group address specifies what multicast groups are proxied.
Metric	Metric for this proxy indicating the priority for the proxy entry. Range is 1 to 255, in which 1 is the highest priority and 255 is the lowest.

Examples

When you add an IGMP proxy on an interface, you can allow a single multicast group or a range of multicast groups to be proxied. An example of each instance is shown below:

Example 1 — This example shows an IGMP proxy that enables a range of multicast groups to be proxied:

Group Address — 225.1.1.0

Mask — 255.255.0.0

This enables a proxy range from 225.1.0.0 to 255.1.255.255

Example 2 — This example shows an IGMP proxy that enables a single multicast group to be proxied:

Group Address — 226.1.1.1

Mask — 255.255.255.255

This enables the interface to proxy the multicast group 226.1.1.1.

Example 3 — This example shows how a more specific IGMP proxy route takes precedence over a less specific route:

Proxy 1 — 225.4.3.0/225.225.225.0 metric 1 1/1/1

Proxy 2 — 225.4.0.0/225.225.0.0 metric 1 1/2/1

If both proxies are configured and a multicast packet to 225.4.3.1 is received, the Cuda 12000 proxies to 1/1/1 but if a packet is received with 225.4.5.1, the Cuda 12000 proxies to 1/2/1.

Deleting IGMP Proxies

To delete an IGMP proxy, follow this procedure:

1. In the **Summary** window, select the interface that includes the proxy you wish to delete.
2. Click the **Proxy** tab. The Proxy window appears.
3. Select the IGMP proxy you wish to delete.
4. Click **Delete**. A window appears to confirm the deletion.

5. Click **Ok** to commit or **Cancel** to exit without saving.

Viewing IP Multicast Routes

To view IP Multicast routes, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **IP** > **Multicast** > **MRoute.**
2. The MRoute window provides this information:

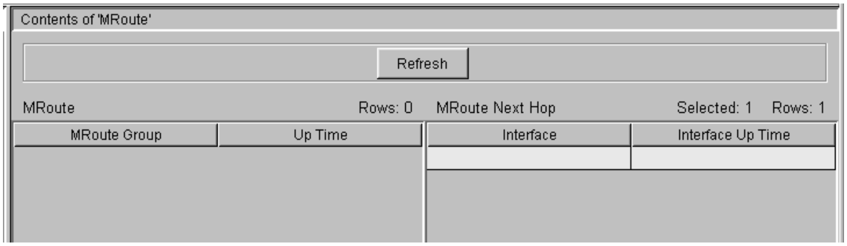
   MRoute Group — IP Multicast group address that contains the multicast routing information.

   Up Time — Time in hours, minutes, and seconds since the multicast routing information was learned.
3. Click the MRoute Group for viewing the next hop information.

   Interface — Interface on which the selected multicast route is learned or joined.

   Interface Up Time — Time in hours, minutes, and seconds since the multicast routing information was learned.

Figure 17-7 MRoute Window


Contents of 'MRoute'

MRoute Rows: 0 MRoute Next Hop Selected: 1 Rows: 1

MRoute Group	Up Time

Interface	Interface Up Time

IV

CABLE MODEM TERMINATION SYSTEMS

18 CONFIGURING AND MONITORING CABLE MODEM TERMINATION SYSTEMS

This chapter explains how to configure the Cuda 12000 for Cable Modem Termination System (CMTS) functionality, and contains statistics for monitoring CMTS operations. The chapter includes the following sections:

- Configuring MAC Interfaces
- Configuring the Downstream Channel
- Configuring Upstream Channels
- Configuring Advanced CMTS Functions
- Viewing Dynamic Services Statistics
- Configuring Modulation Profiles

Overview

The Cuda 12000 performs DOCSIS 1.0 and 1.1 and EuroDOCSIS 1.0 CMTS functionality to provide connectivity and data passing for cable modems over the cable plant. This chapter describes the configuration and monitoring capabilities of the Cuda 12000 DOCSIS and EuroDOCSIS modules.

***Note**: You must have access privileges to the HFC functional area to perform CMTS configuration functions.bb*

CMTS Upstream Frequency Reuse

The Cuda 12000 supports the configuration of upstream channels with the same center frequencies, if the channels are on separate non-combined physical plants. Referred to as upstream frequency reuse, this allows an operator to set aside less of the valuable upstream spectrum for CMTS use. Note, however, that for proper operation such upstream channels must also be configured to have the same channel widths and minislot sizes.

Before You Begin

Before you configure the CMTS, navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **CMTS** > **Interfaces.**

The Interface window provides several configuration tabs and a module information display. The module information panel, located in the top of the window, identifies the interface and the module-type currently selected.

What You See

Figure 18-1 CMTS Folder Window

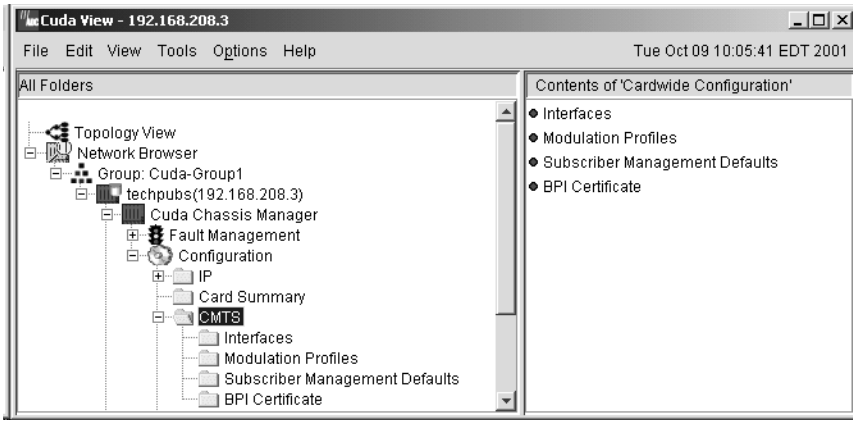
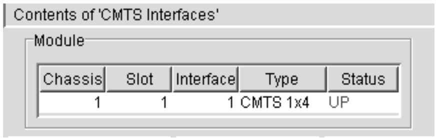


Figure 18-2 Example of a DOCSIS module panel.


Contents of 'CMTS Interfaces'

Module

Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

Parameter Descriptions

This table provides a description of the Module panel

Table 18-1 Description of Module panel fields.

Parameter	Description
Chassis	A unique identifying number you assign to the chassis in the network.
Slot	Slot number in which the DOCSIS or EuroDOCSIS module is installed.
Interface	Chassis/Slot/Interface for the CMTS modules that are currently active
Type	Identifies the module as DOCSIS or EuroDOCSIS, as follows:
Euro-CMTS	Indicates a EuroDOCSIS module.
CMTS	Indicates a DOCSIS module.

Parameter	Description
Status	Indicates the operational status of the module.

Configuring MAC Interfaces

A Media Access Control (MAC) interface is a logical interface implemented within hardware and software. MAC contains one downstream and four upstream channels. Frequencies are assigned for each of the downstream and upstream channels.

Before You Begin

Before you configure MAC interfaces, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **CMTS** > **Interfaces**.
2. Click the **Interfaces** tab. The Interfaces window appears.
3. Select the CMTS interface that you wish to configure.
4. Click the **MAC** tab. The MAC window appears. Use this window to configure the CMTS MAC interface.

MAC Interface Parameters

MAC Interface Parameters are used to initialize the CMTS module. This means that, in addition to saving a configuration on the Cuda 12000 management module, configuration changes must also be applied to the CMTS physical module.To reset a module, refer to Chapter 9, “Module Administration”.

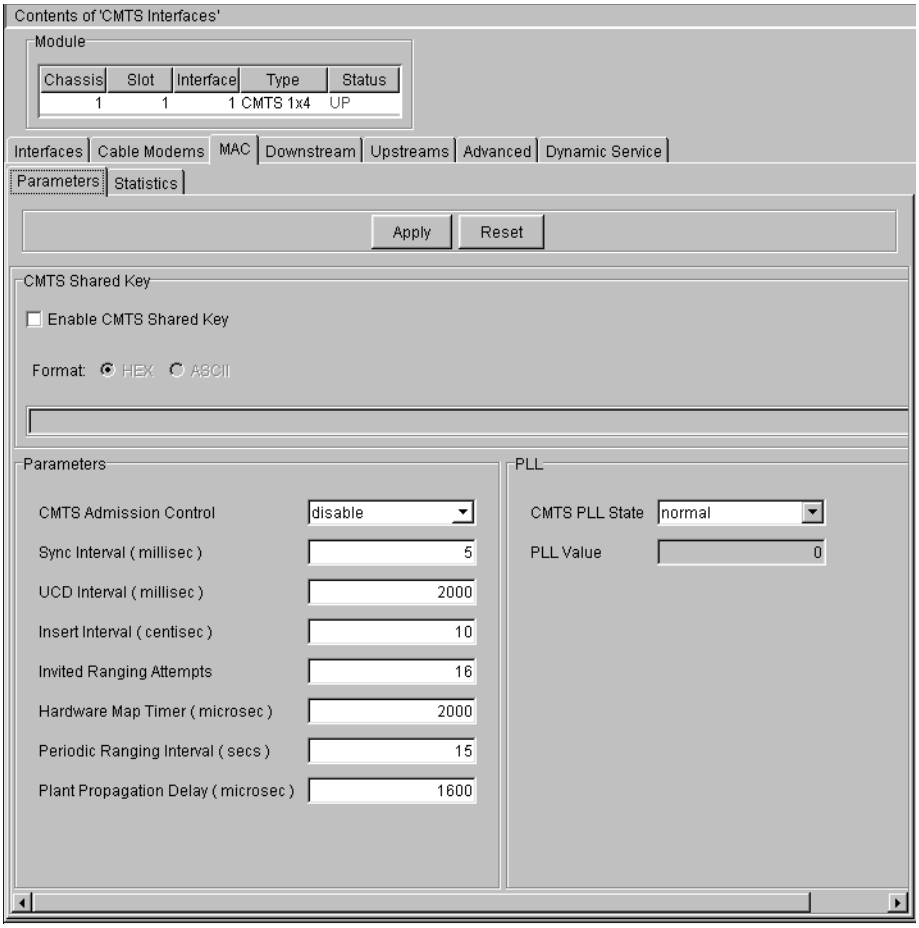
⚠ ***WARNING: MAC parameters affect the performance of the CMTS. It is recommended that configuration is done by an expert-level administrator.***

To configure the MAC interface parameters, follow this procedure:

1. In the MAC window, click the **Parameters** tab. The Parameters window appears.
2. Enter values for the parameters. Refer to Table 18-2.
3. Click **Apply** to commit the information or click **Reset** to return to the default values.

What You See

Figure 18-3 CMTS MAC Interface Parameters Window



Contents of 'CMTS Interfaces'

Module

Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

CMTS Shared Key

□ Enable CMTS Shared Key

Format: ● HEX ○ ASCII

Parameters

CMTS Admission Control	disable
Sync Interval (millisec)	5
UCD Interval (millisec)	2000
Insert Interval (centisec)	10
Invited Ranging Attempts	16
Hardware Map Timer (microsec)	2000
Periodic Ranging Interval (secs)	15
Plant Propagation Delay (microsec)	1600

PLL

CMTS PLL State	normal
PLL Value	0

Parameter Descriptions

This table provides a description of the MAC Interface Parameters window

Table 18-2 .Description of MAC Parameters Window

Parameter	Description
Shared Key	Shared authentication string between CMTS and the provisioning server. Choose the Hex or ASCII option to enter the value in hexidecimal or ASCII format. **Note**: The CMTS Shared Key value must match the Shared Key value used for Provisioning.
CMTS Admission Control	Enable Admission Control to perform the following functions: ■ Allocate HFC interface bandwidth to services flows, and prevents admission of flows when bandwidth is unavailable. ■ Set aside bandwidth for unsolicited grant service (UGS) service flows and UGS with activity detection (UGS/AD) service flows, which are used to transmit voice traffic. By default, Admission Control is disabled.
Sync Interval (millisec)	Sets the time interval between the CMTS transmission of SYNC messages. By default, the SYNC message is sent by the MAC hardware every 5 milliseconds. Acceptable values are 1 to 200 milliseconds.
UCD Interval (millisec)	Sets the time interval between CMTS transmission of Upstream Channel Descriptor for each Upstream Channel. By default, the UCD is sent every 2000 milliseconds. Acceptable values are 1 to 2000 milliseconds.
Insert Interval (centisec)	Specifies the interval between CMTS transmission of Initial Maintenance (IM) intervals. This limits the amount of time during which cable modems can request an upstream frequency from the CMTS and join the network for the first time. By default, the automatic setting is configured at 10 centiseconds. Acceptable values are 5 to 200 centiseconds.
Invited Ranging Attempts	Specifies the maximum number of attempts for the CMTS to attempt ranging a modem as of tolerance or not responding. A value of zero means the system should attempt to range forever. By default, attempts are sent every 16 attempts per ranging period as defined by the Periodic Ranging Timer.

Parameter	Description
Hardware MAP Timer	Sets the time interval between the CMTS transmission of MAP messages for each upstream channel. By default, the setting is for 2000 microseconds. Changing this value causes performance implications.
Periodic Ranging Interval (seconds)	Defines the period during which the CMTS will offer a ranging opportunity to each cable modem. By default, Periodic Ranging is sent every 15 seconds. Acceptable values are 5 to 30 seconds.
Plant Propagation Delay	Specifies the maximum round-trip propagation delay in the cable plant. This value is used to adjust the map lead time. It is recommended that a low value be used to reduce cable modem access delay. For a cable plant of 25 miles, the recommended value is 400. For a cable plant of 100 miles, the recommended value is 1600.
CMTS PLL State	Phase-locked loops (PLL) are circuits that hunt and synchronize to an external signal. For normal CMTS operations, the CMTS PLL State should be set to normal and the PLL Value should be zero.
PLL Value	Read-only. For normal operation of a DOCSIS or EuroDOCSIS module, the PLL value must be zero. A PLL value of non-zero normally indicates a malfunction of the DOCSIS or EuroDOCSIS module. If the PLL Value is non-zero, then set the CMTS PLL State to pllSet. Perform a Refresh, and if the PLL Value continues to display a non-zero value, then this is an indication of a malfunction of the module. Selecting pllSet causes the PLL to immediately start the sequence to hunt and synchronize on an external signal. **NOTE**: pllSet is a debug feature and should be used with caution.

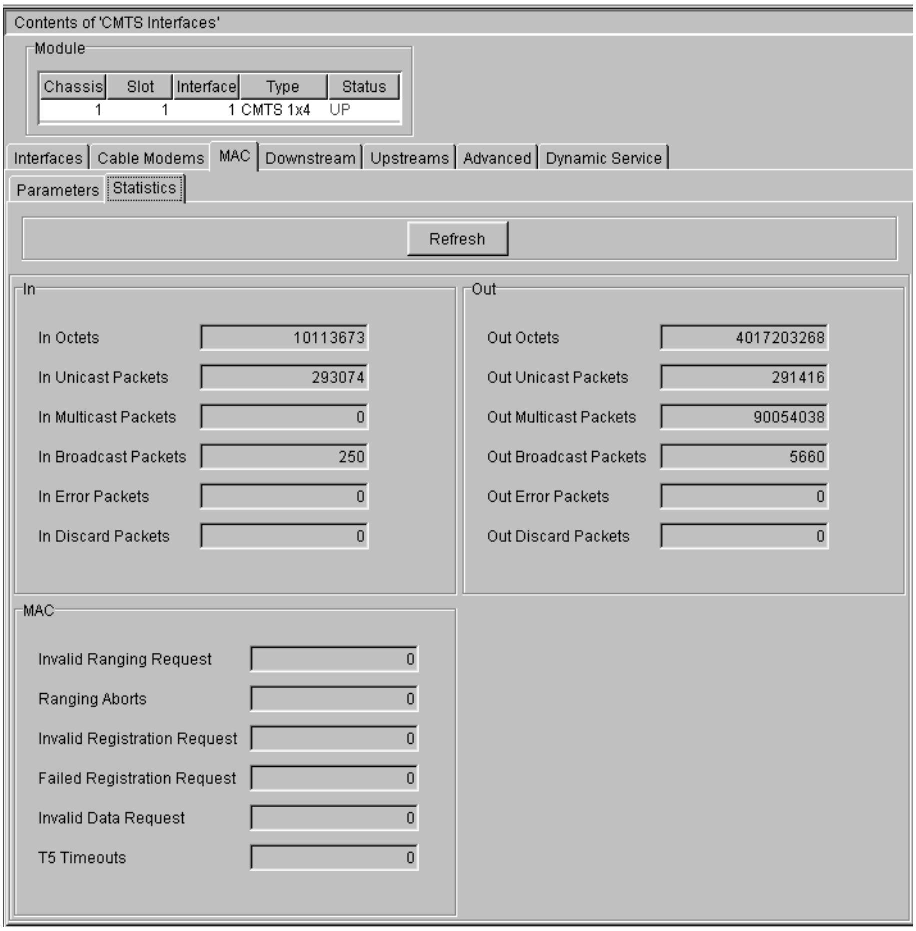
Viewing MAC Interface Statistics

To display the statistics for the MAC Interface level, follow this procedure:

1. In the MAC window, click the **Statistics** tab.
2. Perform a **Refresh** to retrieve the current MAC statistics. Refer to Table 18-3.

What You See

Figure 18-4 MAC Interface Statistics Window



Contents of 'CMTS Interfaces'

Module

Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

In

In Octets	10113673
In Unicast Packets	293074
In Multicast Packets	0
In Broadcast Packets	250
In Error Packets	0
In Discard Packets	0

Out

Out Octets	4017203268
Out Unicast Packets	291416
Out Multicast Packets	90054038
Out Broadcast Packets	5660
Out Error Packets	0
Out Discard Packets	0

MAC

Invalid Ranging Request	0
Ranging Aborts	0
Invalid Registration Request	0
Failed Registration Request	0
Invalid Data Request	0
T5 Timeouts	0

Parameter Descriptions

This table provides a description of the Parameters window

Table 18-3 MAC Statistics Window Parameters.

Parameter	Description
In	Displays statistics for the data received on all upstream channels.
In Octets	Displays the aggregate number of bytes received.

Parameter	Description
In Unicast Packets	Displays the aggregate number of unicast packets received.
In Multicast Packets	Displays the aggregate number of multicast packets received.
In Broadcast Packets	Displays the aggregate number of broadcast packets received.
In Error Packets	Displays the aggregate number of error packets received.
In Discard Packets	Displays the aggregate number of discard packets received.
Out	Displays statistics for the data transmitted from the downstream channel.
Out Octets	Displays the number of bytes transmitted.
Out Unicast Packets	Displays the number of unicast packets transmitted.
Out Multicast Packets	Displays the number of multicast packets transmitted.
Out Broadcast Packets	Displays the number of broadcast packets transmitted.
Out Error Packets	Displays the aggregate number of error packets transmitted.
Out Discard Packets	Displays the aggregate number of discard packets transmitted.
MAC	Displays the state of the upstream channel.
Invalid Ranging Request	Displays the aggregate number of invalid ranging requests received on the MAC interface.
Ranging Aborts	Displays the number of abort range response that were sent by the CMTS.
Invalid Registration Request	Displays the aggregate number of invalid registration requests received.
Failed Registration Request	Displays the aggregate number of failed registration requests from modems.

Parameter	Description
Invalid Data Request	Displays the aggregate number of invalid data requests received.
T5 Timeouts	Displays the number of timeouts waiting for upstream channel change responses.

Configuring the Downstream Channel

The Downstream Channel sends data from the headend to cable modems. Configuring the downstream channel involves setting parameters to maximize the performance of the data transfer. Downstream channel parameters are based on the modulation type for a downstream port on the CMTS.

The downstream center frequency range values and the downstream interleave depth values are different for DOCSIS and EuroDOCSIS. Refer to the descriptions below for detailed configuration information.

Before You Begin

Before you configure downstream channels, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **CMTS** > **Interfaces.**
2. Click the **Interfaces** tab. The Interfaces window appears.
3. Select the CMTS interface that you wish to configure.
4. Click the **Downstream** tab. The Downstream Channel window appears.

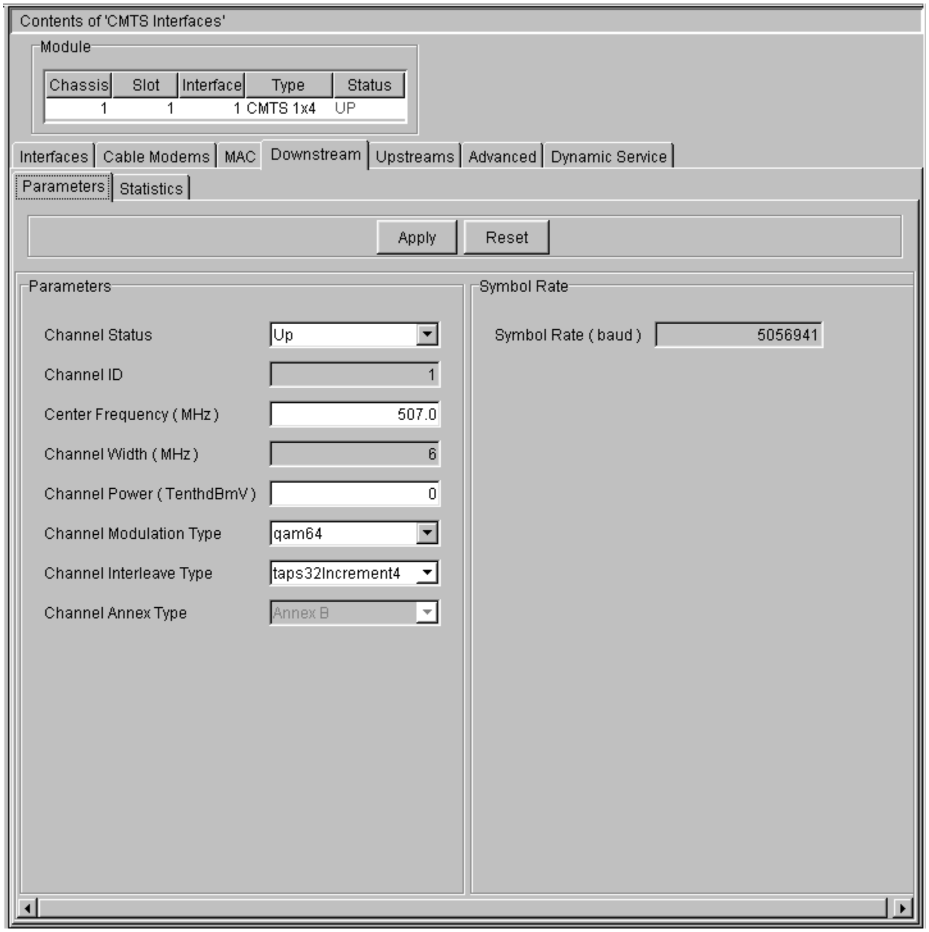
Configuring Downstream Channel Parameters

To configure the downstream channel parameters, follow this procedure:

1. In the Downstream Channel window, click the **Parameters** tab.
2. Enter values for the parameters. Refer to Table 18-5.
3. Click **Apply** to commit the information or click **Refresh** to return to the default values.

What You See

Figure 18-5 Downstream Parameters window.



Contents of 'CMTS Interfaces'

Module

Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

Parameters

Channel Status: Up

Channel ID: 1

Center Frequency (MHz): 507.0

Channel Width (MHz): 6

Channel Power (TenthdBmV): 0

Channel Modulation Type: qam64

Channel Interleave Type: taps32Increment4

Channel Annex Type: Annex B

Symbol Rate

Symbol Rate (baud): 5056941

Parameter Descriptions

Table 18-4 CMTS Downstream Parameters window

Table 18-5 Downstream Window Parameters.

Parameter	**Description**
Channel Status	Normally, displays the current status of the downstream channel, and allows you to set the status of the channel. Up indicates that the channel is active; Down indicates that the channel is inactive. To set the channel to a different state, from the drop-down menu choose the channel state that you want.
Channel ID	Each Cuda 12000 DOCSIS and EuroDOCSIS has a single downstream channel, so the Channel ID is fixed at 1.
Downstream Center Frequency (MHz)	Sets the downstream signal for the RF carrier. Following are default and range values for DOCSIS and EuroDOCSIS configuration. By default, Center Frequency is set at 507.0 MHz. The acceptable values are: ■ DOCSIS — 93.0 MHz to 855 MHz. ■ EuroDOCSIS — 91.0 MHz to 858 MHz.
Channel Width (MHz)	Read-only. The fixed channel width, which is based on DOCSIS and EuroDOCSIS standards and defined by the NTSC channel plan. A DOCSIS module is set at 6 MHz, and a EuroDOCSIS module is set at 8 MHz.
Channel Power (TenthdBmV)	Sets the nominal output transmit power level. By default, Channel Power is set at 550 TenthdBmV. Acceptable values are 0-650.
Downstream Channel Modulation Type	Sets the modulation rate for a downstream port. The CMTS supports the following two modulation types. The options are: ■ qam 64 - sets the interface speed at 30 Mbps ■ qam 256 - sets the interface speed at 40 Mbps **WARNING**: You should know the following about setting Downstream Channel Modulation: Before issuing a downstream modulation change, changes made to any other CMTS parameters should first be persisted. Setting a new downstream modulation to a DOCSIS or EuroDOCSIS module causes the new downstream modulation value to be saved in flash and the module to reset. After the module completes reset, it runs with the new downstream modulation.

Parameter	Description
Downstream Channel Interleave Depth	Sets the FEC Interleaving for the downstream channel. The drop-down menu lists the values that are supported for DOCSIS and EuroDOCSIS. **DOCSIS** — By default, Interleave Depth is set at taps32Increment4. Following are the acceptable values for a DOCSIS module. A higher value improves protection from noise bursts; however, it may increase latency. ■ taps8Increment16 ■ taps16Increment 8 ■ taps32Increment4 ■ taps64Increment2 ■ taps128Increment1 **EuroDOCSIS** — The Interleave Depth for a EuroDOCSIS module must be set at taps12Increment7. NOTE: The first time you install a EuroDOCSIS module you must set the interleave depth, in order for the cable modems to register with the downstream channel.
Downstream Channel Annex Type	Provides support for MPEG framing format for 1x4 DOCSIS and 1x4 EuroDOCSIS modules. The Cuda 12000 automatically detects MPEG framing format, as follows: **Annex A** — Indicates an MPEG framing format for a 1x4 EuroDOCSIS module. **Annex B** — Indicates an MPEG framing format for a 1x4 DOCSIS module.
Symbol Rate	Specifies the MAC symbol rate in symbols per second: ■ qam64 - 5,056,941 symbols per second ■ qam256 - 5,360,537 symbols per second

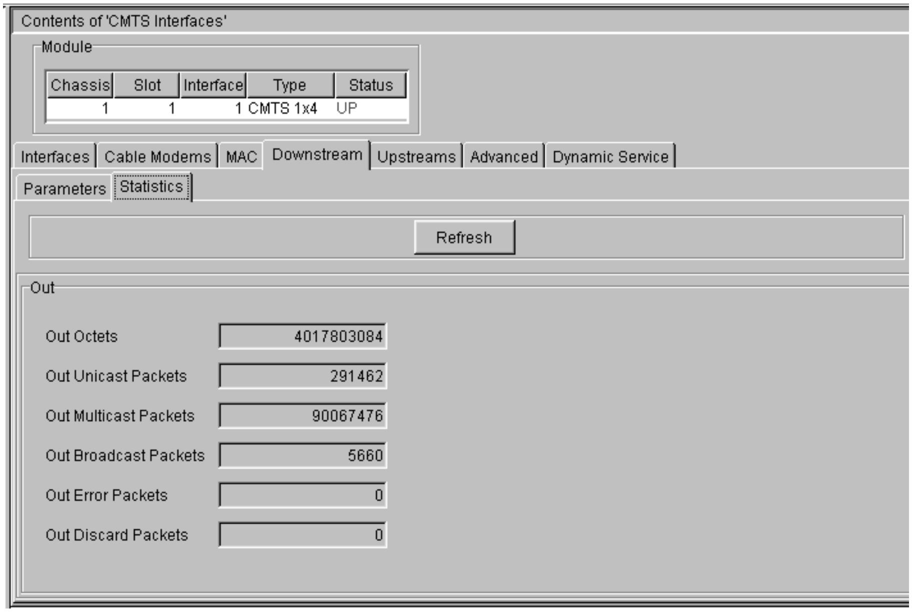
Downstream Channel Statistics

Downstream Channel Statistics monitor the number of bytes transmitted on an interface and the number of packets transmitted on the downstream channel. To display downstream channel statistics, follow this procedure:

1. In the Downstream Channel window, click the **Statistics** tab.
2. Click **Refresh** to update the information. Refer to Table 18-6.

What You See

Figure 18-6 Downstream Statistics Window



Contents of 'CMTS Interfaces'

Module

Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

Out Octets: 4017803084

Out Unicast Packets: 291462

Out Multicast Packets: 90067476

Out Broadcast Packets: 5660

Out Error Packets: 0

Out Discard Packets: 0

Parameter Descriptions

This table provides a description of the Statistics window.

Table 18-6 Downstream Statistics Window Parameters

Parameter	Description
Out Octets	Number of bytes transmitted on the interface.
Out Unicast Packets	Number of unicast packets transmitted on the downstream channel.
Out Multicast Packets	Number of multicast packets transmitted on the downstream channel.
Out Broadcast Packets	Number of broadcast packets transmitted on the downstream channel.
Out Error Packets	Aggregate number of error packets transmitted on the downstream channel.
Out Discard Packets	Aggregate number of discard packets transmitted on the downstream channel.

Configuring Upstream Channels

Upstream channels transfer data from the cable modems to the headend. Data transfer is accomplished in bursts. The Cuda 12000 supports four upstream channels per CMTS module. You must configure each channel independently from the other.

Before You Begin

Before you configure upstream channels, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **CMTS** > **Interfaces.**
2. Click the **Interfaces** tab. The Interfaces window appears.
3. Select the CMTS interface that you wish to configure.
4. Click the **Upstreams** tab. The Upstreams window appears.

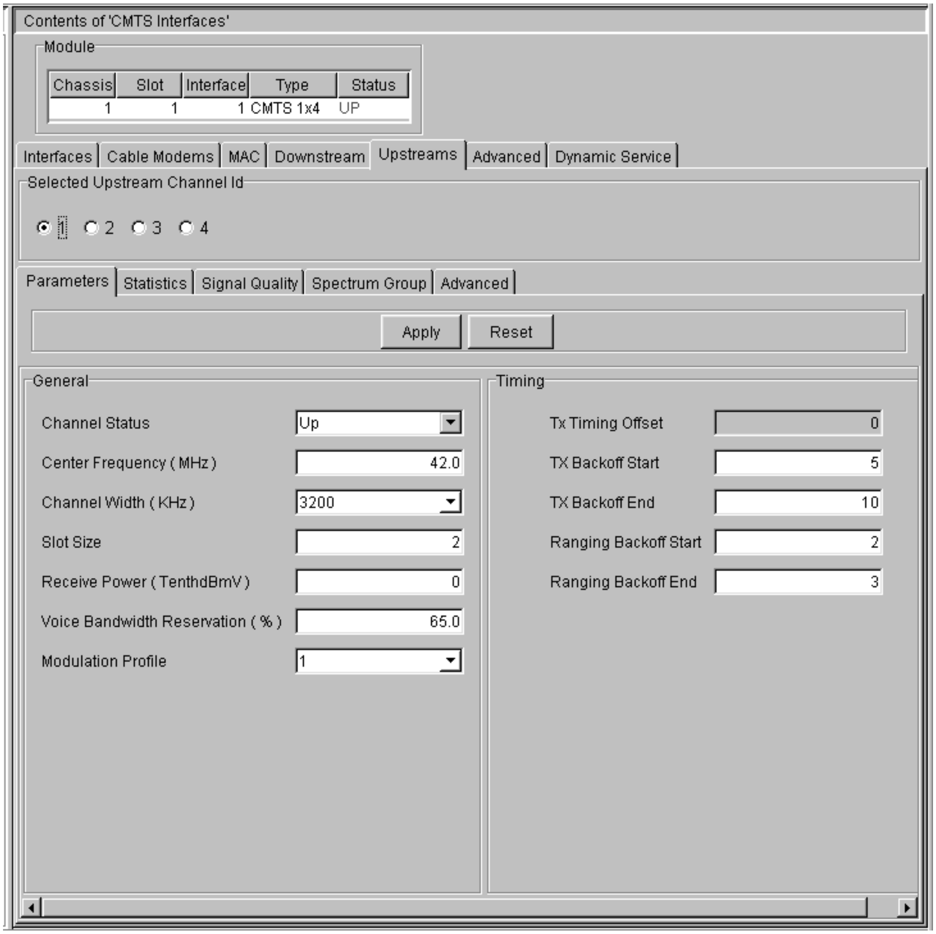
Configuring Upstream Channels Parameters

To configure the upstream channel parameters, follow this procedure:

1. In the Upstreams window, Click the **Parameters** tab.
2. Select the Channel Id that you want to configure, from the Selected Upstream Channel Id menu.
3. Enter values for the parameters. Refer to Table 18-7.
4. Click **Reset** to commit the changes or click **Reset** to return to the previous values.

What You See

Figure 18-7 Upstreams Parameters Window.



Contents of 'CMTS Interfaces'

Module

Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

Selected Upstream Channel Id

● 1 ○ 2 ○ 3 ○ 4

General

Channel Status	Up
Center Frequency (MHz)	42.0
Channel Width (KHz)	3200
Slot Size	2
Receive Power (TenthdBmV)	0
Voice Bandwidth Reservation (%)	65.0
Modulation Profile	1

Timing

Tx Timing Offset	0
TX Backoff Start	5
TX Backoff End	10
Ranging Backoff Start	2
Ranging Backoff End	3

Parameter Descriptions

This table provides a description of the Upstreams Parameters window.

Table 18-7 Description of Upstreams Parameters Window..

Parameter	Description
Channel Status	Normally, displays the current status of the upstream channel, and allows you to set the status of the channel. Up indicates that the channel is active; Down indicates that the channel is inactive. To set the channel to a different state, from the pull-down menu choose the channel state that you want.
Center Frequency (MHz)	Sets the upstream signal frequency for the RF carrier. There is a difference between the frequency range values for DOCSIS and EuroDOCSIS modules. Valid DOCSIS upstream values range from 5.0 - 42.0 MHz. Valid EuroDOCSIS upstream values range from 5.0 - 65.0 MHz.
Upstream Channel Width (kHz)	Sets the upstream channel width in kilohertz (kHz). By default, the Channel Width is set at 3200 kHz (2560 kilosymbols - ksyms). From the drop-down menu, you may choose one of the following acceptable values: ■ 200 kHz (160 ksyms per second) ■ 400 kHz (320 ksyms per second) ■ 800 kHz (640 ksyms per second) ■ 1600 kHz (1280 ksyms per second) ■ 3200 kHz (2560 ksyms per second) The symbol rate is recomputed as follows: symbol rate = channel width/1.25 A higher symbol rate is more susceptible to RF noise and interference. If you use a symbol rate or modulation format beyond the capabilities of your HFC network, there may be packet loss or loss of cable modem connectivity.

Parameter	Description
Slot Size	Number of 6.25 microsecond ticks in each upstream minislot. This depends on one selected channel width, which is automatically set when the user selects an acceptable channel width. By default, the Slot Size is set at 2. **WARNING**: The slot size affects the performance of the CMTS. It is recommended that configuration is done by an expert-level administrator. Following are recommended minislot values for different channel widths: ■ 2 (3200 kHz) ■ 4 (1600 kHz) ■ 8 (800 kHz) ■ 16 (400 kHz) ■ 32 (200 kHz)
Receive Power	Receive power level from the CMTS for the upstream interface from the cable modem. By default, the Receive Power is set at 0, which is the optimal setting for the upstream power level. Acceptable values are -160 to 260 TenthdBmV. The Receive Power is dependent on the selected channel-width.
Voice Bandwidth Reservation (%)	Specify the percentage of bandwidth reserved for UGS and UGS/AD service flows. Acceptable values range from 0.0 to 100.0%. The default is set to 75.0%.
Modulation Profile	Profile Index number that identifies the properties of the Upstream Channel ID.
TX Timing Offset	Read-only. A measure of the maximum round-trip time between a cable modem and the CMTS on this upstream channel.
TX Backoff Start	Sets a fixed start value for initial data backoff on the upstream ports. By default, the TX Backoff Start is set to 5. Acceptable values are 0 to 15.
TX Backoff End	Sets a fixed end value for initial data backoff on the upstream ports. By default, the TX Backoff End is set to 10. Acceptable values are 0 to 15.
Ranging Backoff Start	Sets the fixed start value for range backoff on the upstream ports. By default the value is set to 2. Acceptable values are 0 to 15.

Parameter	Description
Ranging Backoff End	Sets the fixed stop values for range backoff on the upstream ports. By default, the Ranging Backoff End is set to 3. Acceptable values are 0 to 15.

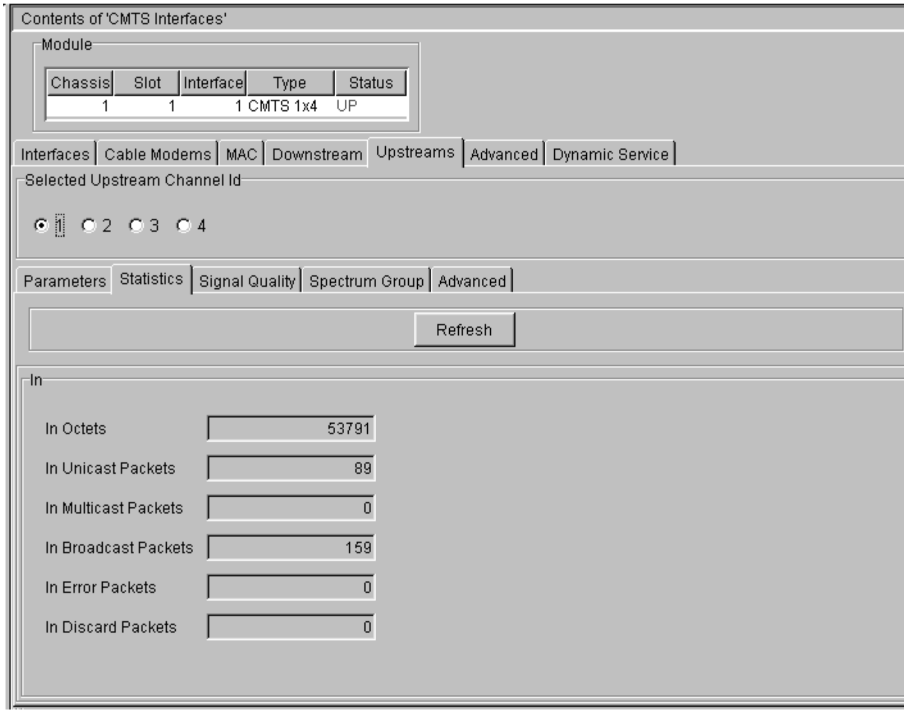
Viewing Upstream Channels Statistics

Upstream Channel Statistics monitor upstream channels. To display the statistics, follow this procedure:

1. In the Upstreams window, click the **Statistics** tab.
2. Select the Channel ID that you want to view, from the **Selected** Upstream Channel Id menu.
3. Click **Refresh** to update the information. Refer to Table 18-8.

What You See

Figure 18-8 Upstreams Statistics Window



Contents of 'CMTS Interfaces'

Module

Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

Selected Upstream Channel Id

● 1 ○ 2 ○ 3 ○ 4

In

In Octets: 53791

In Unicast Packets: 89

In Multicast Packets: 0

In Broadcast Packets: 159

In Error Packets: 0

In Discard Packets: 0

Parameter Descriptions

This table provides a description of the Upstreams Statistics window.

Table 18-8 Upstreams Statistics Window Parameters.

Parameter	Description
In Octets	Number of bytes received on this upstream channel.
In Unicast Packets	Number of unicast packets received on this upstream channel.
In Multicast Packets	Number of multicast packets received on this upstream channel.
In Broadcast Packets	Number of broadcast packets received on this upstream channel.
In Error Packets	Displays the aggregate number of error packets received over all the upstream channels.

Parameter	Description
In Discard Packets	Displays the aggregate number of discard packets received over all the upstream channels.

Viewing Upstream Channels Signal Quality

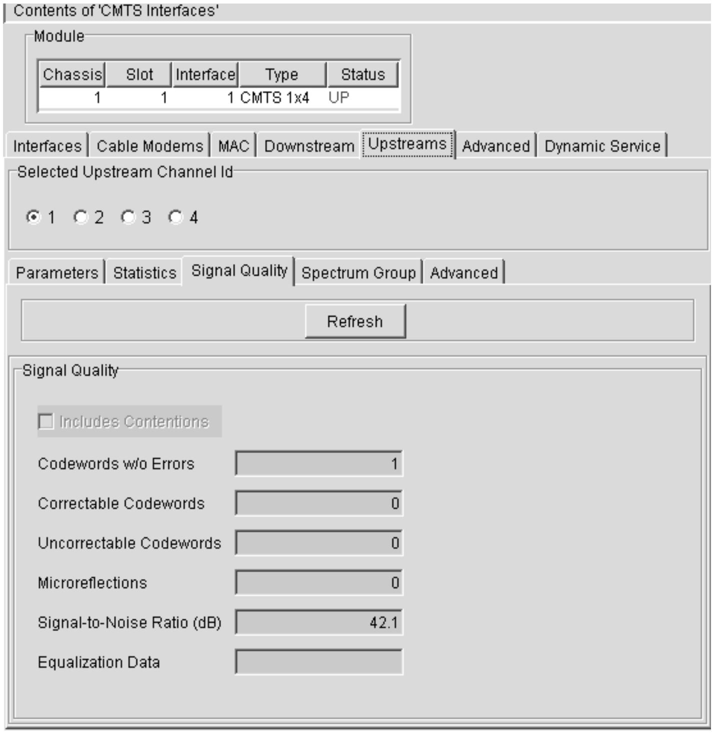
You can monitor signal quality per upstream channel.

To display the signal quality for an upstream channel, follow this procedure:

1. In the Upstreams window, click the **Signal Quality** tab.
2. Select the Channel Id that you want to view from the Selected Upstream Channel Id menu.
3. Click **Refresh** to update the information. Refer to ().

What You See

Figure 18-9 Signal Quality Window



Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

● 1 ○ 2 ○ 3 ○ 4

□ Includes Contentions

Codewords w/o Errors	1
Correctable Codewords	0
Uncorrectable Codewords	0
Microreflections	0
Signal-to-Noise Ratio (dB)	42.1
Equalization Data	

Parameter Descriptions

This table provides a description of the Signal Quality window

Table 18-9 Signal Quality Window Parameters.

Parameter	Description
Codewords w/o Errors	Number of codewords received on this channel without error. This includes all codewords, whether or not they were part of frames destined for this device.
Correctable Codewords	Number of codewords received on this channel with correctable errors. This includes all codewords, whether or not they were part of frames destined for this device.
Uncorrectable Codewords	Number of codewords received on this channel with uncorrectable errors. This includes all codewords, whether or not they were part of frames destined for this device.

Parameter	Description
Microreflections	Total microreflections, including in-channel response as perceived on this upstream channel.
Signal-to-Noise Ratio (dB)	Average signal-to-noise ratio (SNR) on this upstream channel.
Equalization Data	Equalization data should read zero.

About Frequency Hopping (Spectrum Group)

Frequency Hopping provides you with the ability to continuously monitor the quality of the upstream spectrum that is in use to avoid unacceptable error rates due to noise. When the plant quality degrades to an unacceptable level, the operating parameters of the tuned upstream adjusts based on the policy configuration.

The quality of the channel is measured using spectrum quality indicators based on frame error rate. The frame error rate is determined by monitoring the pre and post Forward Error Correction (FEC) rates. The frame error rate is averaged over an amount of time and compared to a configured threshold. When the threshold is exceeded, the currently tuned upstream is considered a degraded spectrum and a decision is made based on the policy for this channel.

Configuring Frequency Hopping

Before you configure frequency hopping, you need to determine to which already configured modulation profile to set the configuration, or, you first need to configure a modulation profile to which you want to configure frequency hopping.

The Cuda 12000 allows you to configure a threshold that is used to determine when the upstream spectrum has degraded to an unacceptable level. This error threshold is a percentage of frames received in error in comparison to the total number of frames received. If FEC is used, then frames in error is the number of pre and post FEC errors. If FEC is not being used, then the number of frames in error is the number of invalid frames received. This error threshold is averaged over an amount of time. When the error threshold is exceeded, the upstream spectrum is considered unacceptable and a change in the operating parameters for the channel is made based on the policies that are specified.

When the error threshold is reached over the configurable time, the upstream frequency and burst profile are changed to those specified in the modulation profile. This allows you to have considerable control and flexibility. For example, when the upstream spectrum for a channel degrades, the initial policy specified may be to keep the tuned center frequency the same and increase FEC, or change from 16 QAM to QPSK in an attempt to improve the use of the spectrum. If the change in operating parameters based on the first policy fails to meet the configured error threshold, then the next policy may be to change to another center frequency in an attempt to find another channel with acceptable quality. Each of these policies is attempted in a round-robin fashion to maintain upstream quality.

Frequency Hopping also allows you to monitor the condition of your plant. Within the Spectrum Group window you may monitor these statistics:

- Error Rate — The percentage of errors.
- Error Count — The number of frames with errors.
- Total Packets — The total number of frames received for each policy.

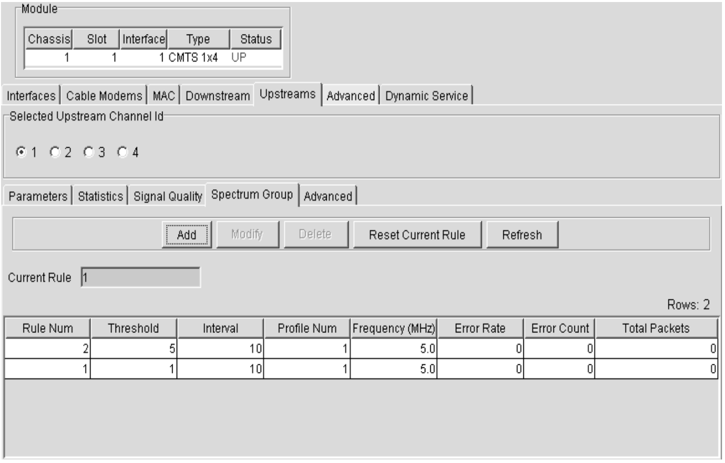
Before You Begin

Before you configure Frequency Hopping, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **CMTS** > **Interfaces.**
2. In the **Interfaces** tab, select the interface that you wish to configure.
3. Click the **Upstreams** tab. The Upstreams configuration window appears.
4. Click the **Spectrum Group** tab. The Spectrum Group window appears.

What You See

Figure 18-10 Spectrum Group Window



Module

Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

Selected Upstream Channel Id

● 1 ○ 2 ○ 3 ○ 4

Current Rule 1

Rows: 2

Rule Num	Threshold	Interval	Profile Num	Frequency (MHz)	Error Rate	Error Count	Total Packets
2	5	10	1	5.0	0	0	0
1	1	10	1	5.0	0	0	0

Parameter Descriptions

This table provides a description of the Spectrum Group window parameters

Table 18-10 Spectrum Group Window Parameters.

Parameter	Description
Rule Num	The number assigned dynamically to the policy.
Threshold	Percentage error threshold for this frequency hopping policy entry.
Interval	Threshold interval, in seconds, for this frequency hopping policy entry.
Profile Num	Upstream burst profile number to be used when error threshold is reached in configured threshold interval time.
Frequency (MHz)	Center frequency value to be used when error threshold is reached in configured threshold interval time.
Error Rate	The percentage of errors.
Error Count	The number of frames with errors.
Total Packets	The total number of frames received for each policy.

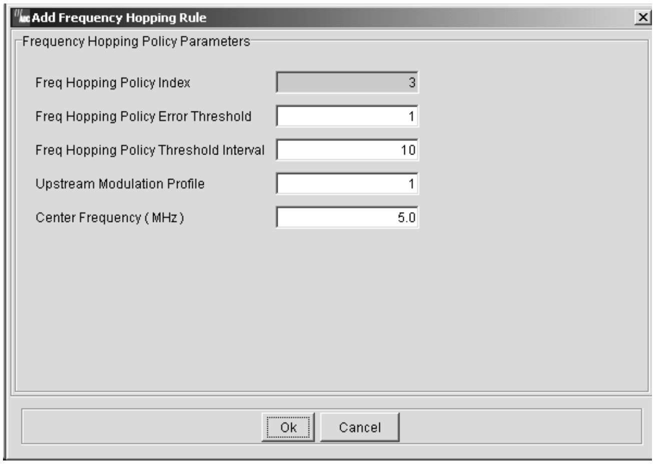
Adding a Policy

For each upstream channel, you may configure up to five policies.

To add a Frequency Hopping policy, follow this procedures:

5. In the **Spectrum Group** window, click **Add**. The Add Frequency Hopping Rule window appears.
6. Enter values for the parameters. Refer to Table 18-23.
7. Click **Ok** to commit the changes or click **Cancel** to exit without saving.
8. Click **Refresh** to update the window.

Figure 18-11 Add Frequency Hopping Rule Window



Add Frequency Hopping Rule

Frequency Hopping Policy Parameters

Freq Hopping Policy Index: 3

Freq Hopping Policy Error Threshold: 1

Freq Hopping Policy Threshold Interval: 10

Upstream Modulation Profile: 1

Center Frequency (MHz): 5.0

Parameter Descriptions

This table provides a description of the Add Frequency Hopping Rule window parameters

Table 18-11 Frequency Hopping Configuration Parameters.

Parameter	Description
Freq Hopping Policy Index	Read only. The rule number assigned to this policy.
Freq Hopping Policy Error Threshold	Percentage error threshold for this frequency hopping policy entry. By default, error threshold is set to 1.

Parameter	Description
Freq Hopping Policy Threshold Interval	Threshold interval, in seconds, for this frequency hopping policy entry. By default, threshold interval is set to 10.
Freq Hopping Profile Number	Modulation profile number to be used when error threshold is reached in configured threshold interval time.
Center Frequency (MHz)	Center frequency value to be used when error threshold is reached in configured threshold interval time. By default, center frequency is set to 5 Mhz.

Modifying a Policy

To modify a Frequency Hopping policy, follow this procedure:

1. In the **Spectrum Group** window, select the entry you wish to modify.
2. Click **Modify**. The Modify Frequency Hopping Rule window displays.
3. Modify the required parameters. Refer to Table 18-23.
4. Click **Ok** to commit the changes or click **Cancel** to exit without saving.

Deleting a Policy

To delete a Frequency Hopping policy, follow this procedure:

1. In the **Spectrum Group** window, select the entry that includes the policy you want to delete.
2. Click **Delete**. A window displays to confirm
3. Click **Yes** to delete the policy or click **Cancel** to exit without deleting.

Resetting a Policy

You may change the specific configuration of a current rule to the default configuration.

To use the default configuration for a current rule, follow this procedure:

1. In the **Spectrum Group** window, select the entry you wish to change.
2. Click the Reset Current Rule button. *Note that a confirmation window does not display, and the configuration is changed immediately to the default values.*

Advanced Configuration for Upstream Channels

The advance configuration features for Upstream Channels allows the you to fine tune the performance of the upstream channel to match one specific requirement or one cable plant. Advanced configuration includes setting the upstream channel parameters for mapping and ranging.

⚠ ***WARNING: Advanced configuration affects the performance of the CMTS. It is recommended that configuration is performed by an expert-level administrator.***

Setting Map Parameters

Channel Map allows you to fine tune MAP generation for the upstream channel.

To set the map parameters, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **CMTS** > **Interfaces.**
2. In the **Interfaces** tab, select the interface that you wish to configure.
3. Click the **Upstreams** tab. The Upstreams configuration window appears.
4. In the Upstreams window, select the channel you want to configure, from the Selected Upstream Channel Id menu.
5. Click the **Advanced** tab.

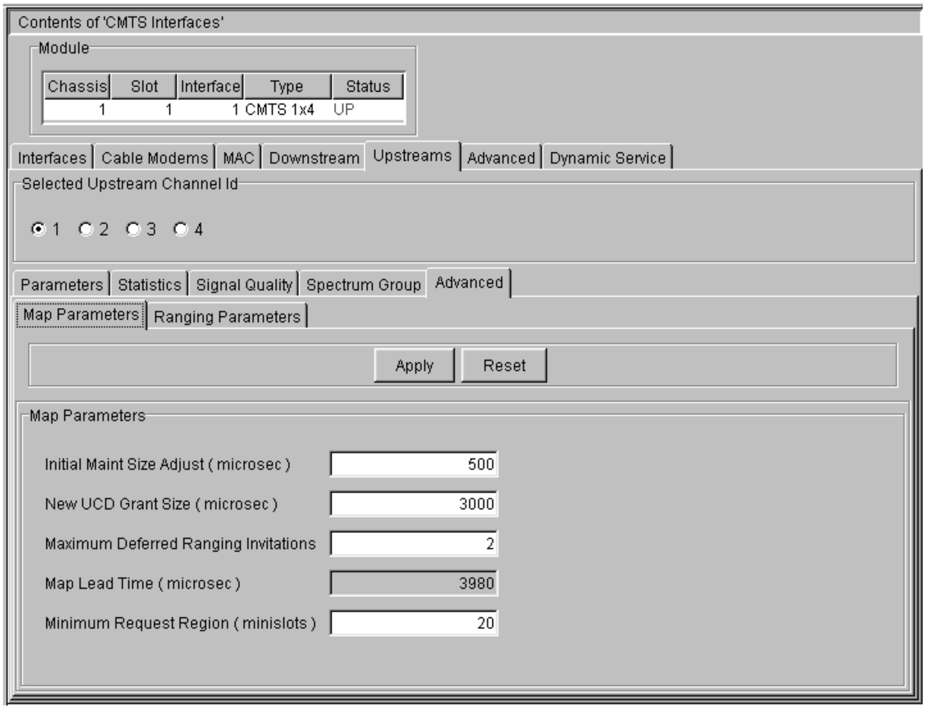
6 Click the **Map Parameters** tab.

7 Enter values for the parameters. Refer to Table 18-12.

8 Click **Apply** to commit the information or click **Reset** to return to the default values.

What You See

Figure 18-12 MAP Parameters window.



Contents of 'CMTS Interfaces'

Module

Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

Selected Upstream Channel Id

● 1 ○ 2 ○ 3 ○ 4

Map Parameters

Initial Maint Size Adjust (microsec): 500

New UCD Grant Size (microsec): 3000

Maximum Deferred Ranging Invitations: 2

Map Lead Time (microsec): 3980

Minimum Request Region (minislots): 20

Parameter Descriptions

This table provides a description of the Map Parameters window.

Table 18-12 Map Parameters Window

Parameter	Description
Initial Maint Region Size (microsec)	Size of the upstream channel Initial Maintenance (IM) contention region. Maps with Initial Maint regions are sent periodically. By default, Initial Maint Contention Region Size is set at 500.
New UCD Grant Size (microsec)	Upstream Channel Description (UCD) grant size change, specifies the grant size as zero sid. This functions as a delay for cable modems to digest the new UCD. By default, New UCD Grant Size is set at 3000.

Table 18-12 Map Parameters Window (continued)

Parameter	**Description**
Maximum Deferred Ranging Invitations	Maximum number of deferred ranging invitations. By default, Maximum Deferred Ranging Invitations is set at 2.
Map Lead Time (microsec)	Read-Only. Map lead time, in milliseconds. Lead time must be estimated and added to map start time in order that the subscriber modem map receives and processes the map before it is out of date.
Minimum Request Region	Minimum size, in minislots, for request contention region. The default is 20.

Setting Ranging Parameters

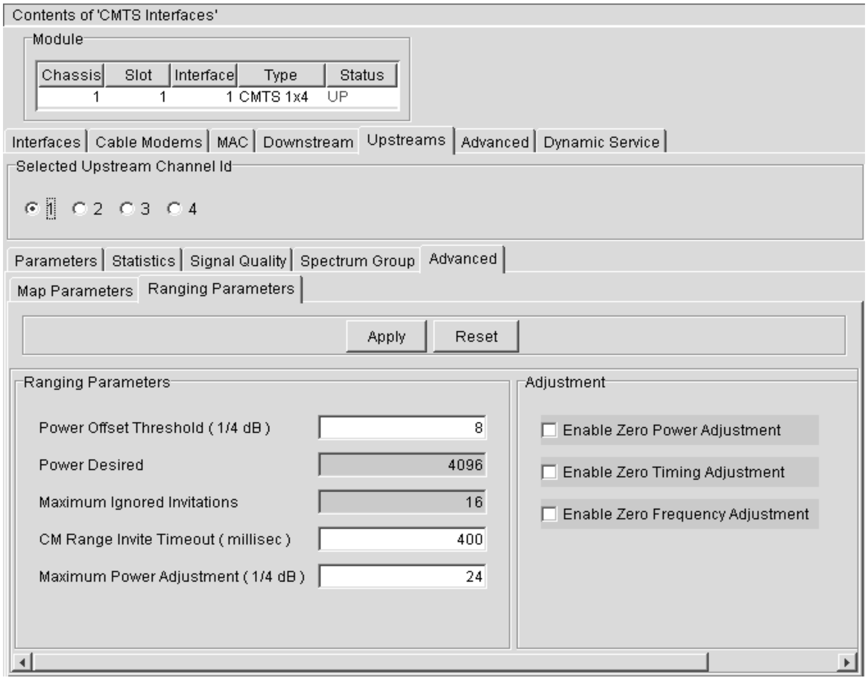
Ranging parameters allow you to fine tune how cable modems adjust power levels during one ranging process.

To configure the ranging parameters, follow this procedure:

1. In the Upstreams, click **Advanced** tab.
2. Click the **Ranging Parameters** tab.
3. Select the channel ID that you want to configure, from the Selected Upstream Channel Id menu.
4. Enter values for the parameters. Refer to Table 18-13.
5. Click **Apply** to commit the information or click **Reset** to return to the default values.

What You See

Figure 18-13 Ranging Parameters window.



Contents of 'CMTS Interfaces'

Module

Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

Selected Upstream Channel Id

● 1 ○ 2 ○ 3 ○ 4

Ranging Parameters

Power Offset Threshold (1/4 dB)	8
Power Desired	4096
Maximum Ignored Invitations	16
CM Range Invite Timeout (millisec)	400
Maximum Power Adjustment (1/4 dB)	24

Adjustment

☐ Enable Zero Power Adjustment

☐ Enable Zero Timing Adjustment

☐ Enable Zero Frequency Adjustment

Parameter Descriptions

This table provides a description of the Ranging Parameters window.

Table 18-13 Ranging Parameters Window

Parameter	Description
Power Offset Threshold (dB)	Specify in 1/4 dB units. If power level offset reported by MAC chip is less than or equal to this threshold value, then power level adjustment may be stopped. By default, Power Offset Threshold is set at 8.
Power Desired	Read-only. This is used as a reference when computing power adjustment.
Maximum Rang ing Invitations	Read-only. Maximum ranging invitations that a CM may ignore before being considered quiet.

Table 18-13 Ranging Parameters Window (continued)

Parameter	Description
CM Range Invite Timeout (millisec)	Minimum time allowed for a cable modem following receipt of a RNG-RSP, before it is expected to reply to an invitation to range request in milliseconds. By default, the CM Range Invite Timeout is set at 400 milliseconds.
Maximum Power Adjustment (1/4 dB)	Maximum adjustment permitted on a single Range Response message, specified in 1/4 dB units. By default, Maximum Power Adjustment is set at 6 dB.
Enable Zero Power Adjustment	If enabled, the power adjustment field in the range response message is unconditionally set to 0. Useful for debugging. By default, Enable Zero Power Adjustment is disabled.
Enable Zero Timing Adjustment	If enabled, the timing adjustment item in range response message is unconditionally set to 0. Useful for debugging. By default, Enable Zero Timing Adjustment is disabled.
Enable Zero Frequency Adjustment	If enabled, the frequency adjustment item in range response message is unconditionally set to 0. Useful for debugging. By default, Enable Zero Frequency Adjustment is disabled.

Configuring Advanced CMTS Functions

Advanced CMTS configuration includes the following functions:

- Configuring the Baseline Privacy Interface
- Configuring Flap Control
- Configuring CM Offline Control
- Viewing QoS Profile Summaries

WARNING: Advanced configuration affects the performance of the CMTS. It is recommended that configuration is performed by an expert-level administrator.

Configuring the Baseline Privacy Interface

The Baseline Privacy Interface (BPI) protocol provides cable modems with data privacy across the Hybrid Fiber-Coaxial (HFC) network by encrypting traffic between cable modems and the CMTS. In addition, BPI provides authorization parameters and traffic encryption keys that secure traffic between cable modems and the CMTS.

For more information about managing BPI, refer to Chapter 20, "Managing Cable Modems" on page 555.

Within Advanced CMTS configuration, configuring BPI includes the following tasks:

- Configuring Authorization and Traffic Encryption Keys.
- Configuring IP Multicast Address Mapping
- Configuring Multicast SAID Authorization

Before You Begin

Before you begin to configure BPI, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **Interfaces.**
2. Click the **Interfaces** tab. Select the interface that you want to configure.
3. Click the **Advanced** tab.
4. Click the **BPI Parameters** tab.

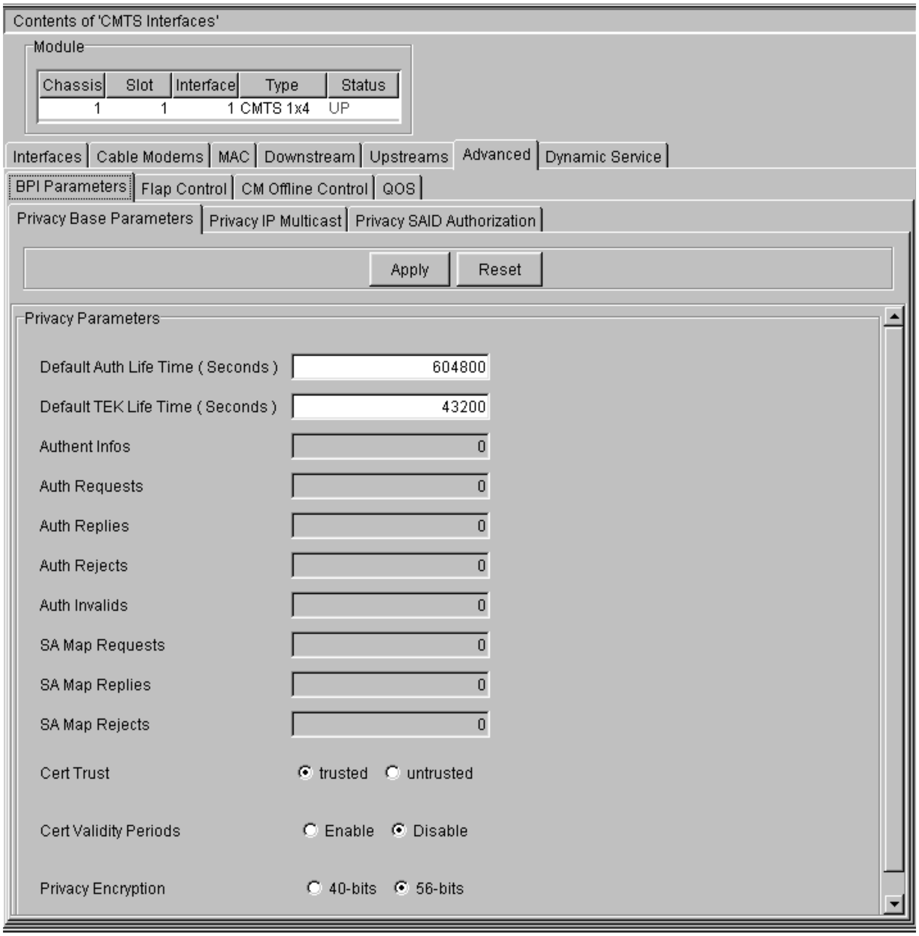
Configuring Authorization and Traffic Encryption Keys

You can configure and view lifetime in seconds for all existing authorization and Traffic Encryption Keys (TEKs), for a specified interface. Follow this procedure:

1. In the BPI Parameters window, click the **Privacy Base Parameters** tab.
2. Enter values for the parameters. Refer to Table 18-14.
3. Click **Apply** to persist the information or click **Reset** to return to the default values.

What You See

Figure 18-14 Privacy Base Parameters Window.



Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

Default Auth Life Time (Seconds)	604800
Default TEK Life Time (Seconds)	43200
Authent Infos	0
Auth Requests	0
Auth Replies	0
Auth Rejects	0
Auth Invalids	0
SA Map Requests	0
SA Map Replies	0
SA Map Rejects	0
Cert Trust	● trusted ○ untrusted
Cert Validity Periods	○ Enable ● Disable
Privacy Encryption	○ 40-bits ● 56-bits

Parameter Descriptions

This table provides a description of the Privacy Base Parameters window.

Table 18-14 Privacy Base Window Parameters

Parameter	**Description**
Default Auth Life Time (Seconds)	Default lifetime, in seconds, the CMTS assigns to a new authorization key. The range is 1 to 6048000 seconds.

Parameter	Description
Default TEK Life Time (Seconds)	Default lifetime, in seconds, the CMTS assigns to a new Traffic Encryption Key (TEK). The range is 1 to 604800 seconds.
Authent Infos	Read only. Number of times the CMTS receives an authentication message from any cable modem.
Auth Requests	Read only. Number of times the CMTS receives an authorization request message from any cable modem.
Auth Replies	Read only. Number of times the CMTS transmits an authorization reply message to any cable modem.
Auth Rejects	Read only. Number of times the CMTS transmits an authorization reject message to any cable modem.
Auth Invalids	Read only. Number of times the CMTS transmits an authorization invalid message to any cable modem.
SA Map Requests	Read only. Number of times the CMTS receives an SA map request message from any cable modem.
SA Map Replies	Number of times the CMTS transmits an SA map reply message to any cable modem.
SA Map Rejects	Number of times the CMTS transmits an SA map reply message to any cable modem.
Cert Trust	Default trust of all new self-assigned manufacturer certificates. The options are:
Trusted	Indicates a valid certificate.
Untrusted	Indicates an invalid certificate. The default is set to untrusted.
Cert Validity Periods	Indicates when certificates are checked for validity. The options are:
Enable	All certificates have the validity checked against the current time of day.
Disable	Certificates do not have the validity checked against the current time of day.
Privacy Encryption	Configures the interface for baseline privacy encryption. The options are:
40-bits	Encryption is set at 40-bits.
56-bits	Encryption is set at 56-bits.

Configuring IP Multicast Address Mapping

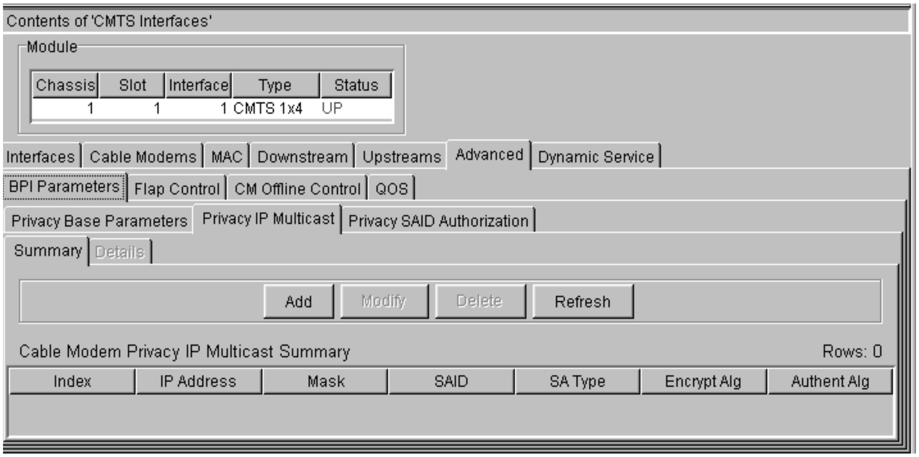
You can configure and display an IP multicast address mapping entry for a CMTS MAC interface.

Configuring involves adding, modifying and deleting mapping entries. To configure IP multicast mapping, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **Interfaces.**
2. Click the **Interfaces** tab. Select the interface that you want to configure.
3. Click the **Advanced** tab.
4. Click the **BPI Parameters** tab.
5. In the BPI Parameters window, click the **Privacy IP Multicast** tab.
6. Click the **Summary** tab.The Privacy IP Multicast Summary window appears. Refer to Table 18-15.
7. Click **Refresh** to update the information.

What You See

Figure 18-15 Privacy IP Multicast window.



Contents of 'CMTS Interfaces'

Module

Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

Cable Modem Privacy IP Multicast Summary Rows: 0

Index	IP Address	Mask	SAID	SA Type	Encrypt Alg	Authent Alg

Parameter Descriptions

This table provides a description of the Privacy IP Multicast window.

Table 18-15 Privacy IP Multicast Summary Window Parameters

Parameter	Description
Index	Identifies the multicast mapping entry.
IP Address	The Class D IP address of the multicast group, to which the security association specified by the SAID is applied.
Mask	The mask that is used with the multicast group address.
SAID	The multicast SAID used in this IP Multicast address mapping entry.
SA Type	The security association type.
Encrypt Alg	The encryption algorithm.
Authent Alg	At this time, only a value of **none** is supported.
SA Map Requests	Read only. Number of times the CMTS receives an SA map request message for this IP address.
SA Map Replies	Number of times the CMTS transmits an SA map reply message for this IP address.
SA Map Rejects	Number of times the CMTS transmits an SA map reply message for this IP address.
Error Code	Error code in the most recent SA map reject message sent in response to an SA map request for this IP address. The options are:
Unknown	Last error code value was zero.
None	No SA map reject message has been received since reboot.
Error String	Display string in the most recent SA map reject message sent in response to an SA map request message for this IP address. It is a zero if no SA map reject message is received since last reboot.

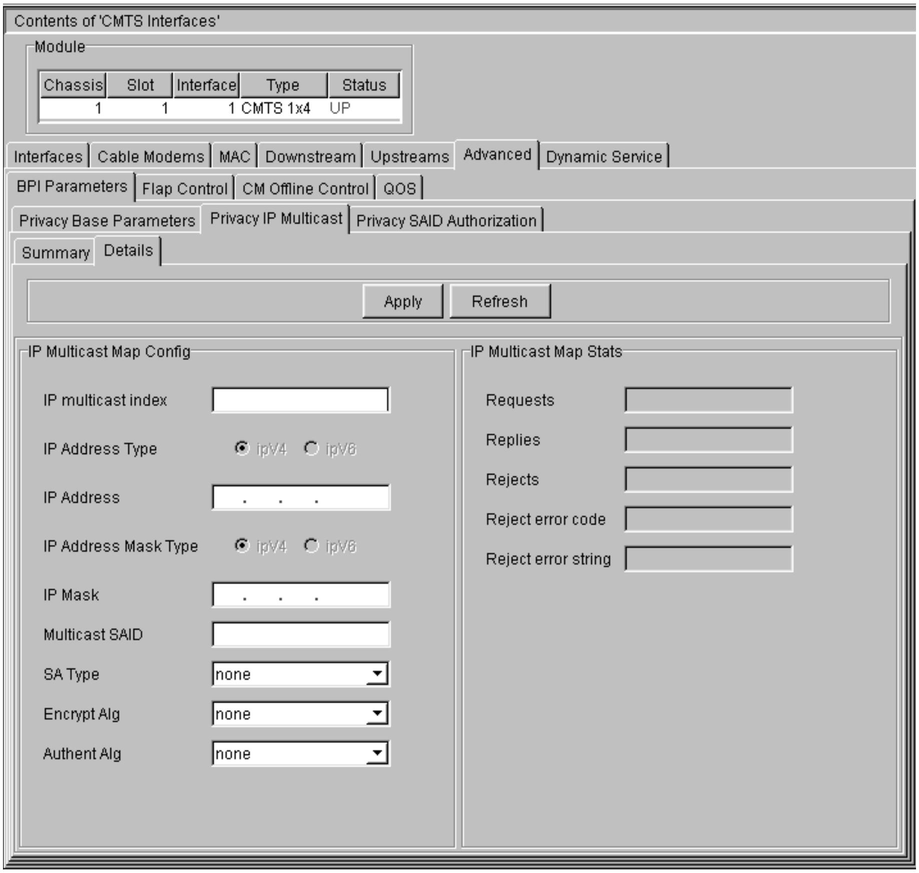
Adding a Privacy IP Multicast Entry

To add an IP Multicast entry, follow this procedure.

1. In the BPI Parameters window, click the **Privacy IP Multicast** tab. The Privacy IP Multicast window appears.
2. Click **Add**. The **Details** window appears.
3. Enter the required information. Refer to Table 18-16.
4. Click **Apply** to commit the changes.

What You See

Figure 18-16 Privacy IP Multicast Details Window. *Note that the window is divided into two panels: IP Multicast Map Config and IP Multicast Map Stats*.



Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

IP multicast index

IP Address Type ● ipV4 ○ ipV6

IP Address . . .

IP Address Mask Type ● ipV4 ○ ipV6

IP Mask . . .

Multicast SAID

SA Type none

Encrypt Alg none

Authent Alg none

Parameter Descriptions

This table provides a description of the Detail window parameters.

Table 18-16 Privacy IP Multicast Details Window Parameters

Parameter	Description
IP Multicast Index	Specify an index that identifies the multicast mapping entry. Acceptable values are 1 to 10000.
IP Address Type	Specify the internet address for an IP multicast address. At this time, only **ipV4** is supported.
IP Address	Specify the Class D IP address of the multicast group to which you are applying the security association specified by the SAID.
IP Address Mask Type	Specify the internet address for an IP multicast mask. At this time, only **ipV4** is supported.
IP Mask	Specify the mask that can be used with a single multicast group address; or, specify a multicast address range. For example: ■ For a single multicast group address of 239.2.2.2, specify a mask of 255.255.255.255. ■ For a multicast address range with an address of 239.1.0.0 and a mask of 255.255.0.0, the SA applies to all multicast groups within 239.1.0.0.
Multicast SAID	Specify the multicast SAID to be used in the multicast address mapping entry. Acceptable values are 8192 to 16383.
SA Type	Specify one of the following security association types: ■ none - No security association. ■ primary - Primary Security Association. This is tied to a single cable modem and is established when that cable modem completes CMTS MAC registration. ■ static - Static Security Association, which is provisioned within the CMTS. ■ dynamic - Dynamic Security Association. This is established and eliminated with the response to the initiation and termination of specific (downstream) traffics flows. Both static and dynamic SA types may be shared by multiple cable modems.

Parameter	Description
Encrypt. Alg	Specify one of the following encryption algorithms: ■ none - no encryption. ■ des56cbcMode - a 56-bit DES packet data encryption. ■ des40cbcMode - a 40-bit DES packet data encryption.
Authent. Alg	Specify the authentication algorithm. At this time, only a value of none is supported.
Requests	Read only. The number of times the CMTS has received an SA Map Request message for this IP.
Replies	Read only. The number of times the CMTS has transmitted an SA Map Reply message for this IP
Rejects	Read only. The number of times the CMTS has transmitted an SA Map Reject message for this IP.
Reject error code	The enumerated description of the Error-Code in the most recent SA Map. The Reject message sent in response to a SA Map Request for this IP. It has value unknown(2) if the last Error-Code value was 0, and none(1) if no SA MAP Reject message has been received since reboot
Reject Error String	The Display-String in the most recent SA Map Reject message sent in response to an SA Map Request for this IP. It is a zero length string if no SA Map Reject message has been received since reboot.

Modifying a Privacy IP Multicast Entry

You may modify IP multicast map entries. To modify entries, follow this procedure:

1. In the BPI Parameters window, click the **Privacy IP Multicast** tab. The Privacy IP Multicast window appears.
2. Click the **Summary** tab. Select the row that includes the entry that you want to change.
3. Click **Modify**. The **Details** window appears.
4. Modify the required information. Refer to Table 18-16.
5. Click **Ok** to commit the changes or click **Cancel** to exit without changes.

Deleting a Privacy IP Multicast Entry

You may delete IP multicast map entries. To delete entries, follow this procedure:

1. In the BPI Parameters window, click the **Privacy IP Multicast** tab. The Privacy IP Multicast window appears.
2. Click the **Summary** tab. Select the row that includes the entry that you want to delete.
3. Click **Delete.**
4. Click **Ok** to delete the entry; or click **Cancel** to exit without deleting.

Configuring Multicast SAID Authorization

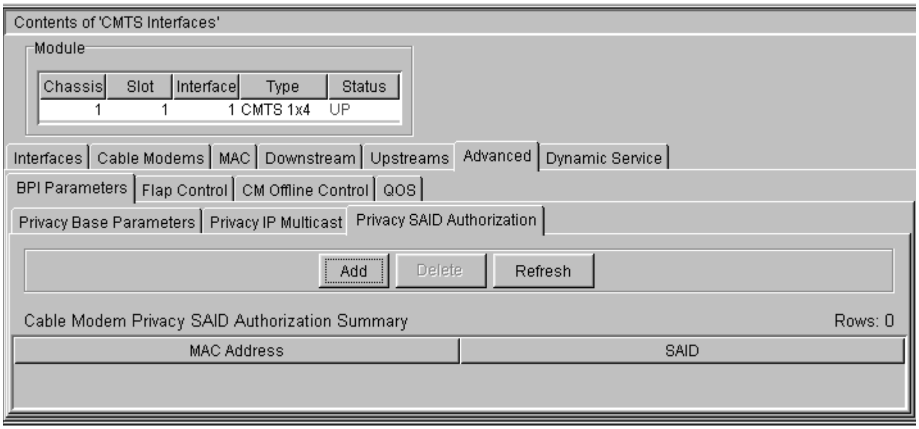
You may configure and display the associated multicast SAID authorization for an interface. Configuration involves adding and deleting SAID authorization entries.

To configure multicast SAID Authorization, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **Interfaces.**
2. Click the **Interfaces** tab. Select the interface that you want to configure.
3. Click the **Advanced** tab.
4. Click the **BPI Parameters** tab.
5. In the BPI Parameters window, click the **Privacy SAID Authorization** tab. The Cable Modem Privacy SAID Authorization Summary window appears. Refer to Table 18-15.
6. Click **Refresh** to update the information.

What You See

Figure 18-17 Cable Modem Privacy SAID Authorization Summary window.



Contents of 'CMTS Interfaces'

Module

Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

Cable Modem Privacy SAID Authorization Summary Rows: 0

MAC Address	SAID

Parameter Descriptions

This table describes the parameters in the summary window:

Table 18-17 Cable Modem Privacy SAID Authorization Summary window parameters:

Parameter	Description
MAC Address	MAC address of the cable modem to which the multicast SAID authorization applies.
SAID	Multicast SAID used in this IP Multicast address mapping entry.

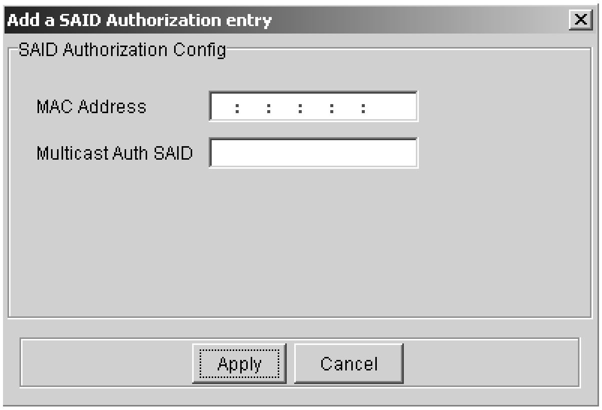
Adding a Multicast SAID Authorization Entry

To add an entry, follow this procedure:

1. In the BPI Parameters window, click the **Privacy SAID Authorization.**
2. In the summary window, click **Add**. The Add a SAID Authorization entry window appears.
3. Enter the parameter values. Refer to Table 18-17.
4. Click **Apply** to commit the changes or click **Cancel** to exit without adding.

What You See

Figure 18-18 Add a SAID Authorization entry window.



Deleting a SAID Authorization Entry

To delete a SAID Authorization entry, follow this procedure:

1. In the BPI Parameters window, click the **Privacy SAID Authorization** tab. The Cable Modem Privacy SAID Authorization Summary window appears.
2. Select the entry you wish to delete.
3. Click **Delete**. A confirmation window appears.
4. Click **Ok** to commit the changes or click **Cancel** to cancel the deletion.

Configuring Flap Control

Flap Control configuration allows you to set parameters for table size and entry thresholds. For information about displaying the flap list, refer to Chapter 20, “Managing Cable Modems”, on page 555.

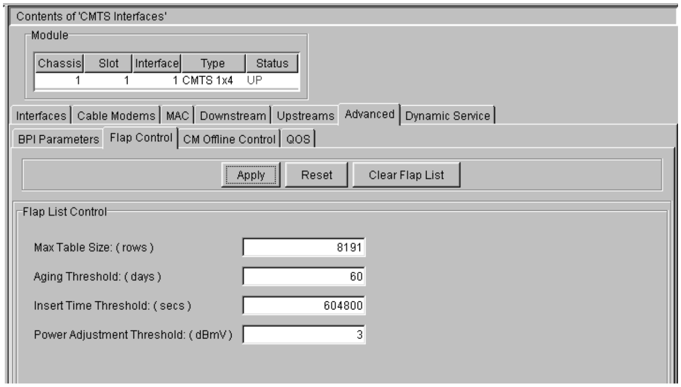
To configure Flap Control, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **Interfaces.**
2. Click the **Interfaces** tab. Select the interface that you want to configure.
3. Click the **Advanced** tab.

4. Click the **Flap Control** tab. The Flap List Control window appears.
5. Enter values for the parameters. Refer to Table 18-18.
6. Click **Apply** to commit the configuration; or, click **Reset** to set the fields to the default values.

What You See

Figure 18-19 Flap List Control Window



Contents of 'CMTS Interfaces'

Module

Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

Flap List Control

Max Table Size: (rows) 8191

Aging Threshold: (days) 60

Insert Time Threshold: (secs) 604800

Power Adjustment Threshold: (dBmV) 3

Parameter Descriptions

This table describes the parameters that you configure for Flap Control.

Table 18-18 Flap Control Parameters

Parameter	Description
Max Table Size: (rows)	Specify the maximum number of entries (cable modems) in the flap list. By default, the table size is set to 8192. Acceptable values are 0 to 8192.
Aging Threshold: (days)	Specify the number of days to age the cable modem from the flap list table. By default, aging is set to 60 days. Acceptable values are 1 to 60 days. *Note that setting the aging threshold to zero results in cable modems never being aged from the table.*

Parameter	Description
Insert Time Threshold: (secs)	Specify a threshold that controls the operation of a flapping modem detector. When the link establishment rate of a modem is shorter than the period defined by this parameter, the modem is placed in the flap list. By default, Insert Time Threshold is set at 604800 seconds. Acceptable values are 0 to 604800 seconds. *Note that setting insert time to zero results in cable modems never being inserted in the flap list table, due to short link establishment times*.
Power Adjustment Threshold: (dBmV)	Specify the number of flap list events. By default, Power Adjustment Threshold is set at 3. Acceptable values are 1 to 10 dBmv. *Note that setting power adjustment to zero results in cable modems never being inserted in the flap list table, due to power adjustments*.

Clearing Flap Lists

You may delete all entries in the flap list table on a specific cable interface.

To clear the flap list, within the Flap List Control window click the **Clear Flap List** button. Note that a confirmation window is not displayed, and the entire flap list table is cleared immediately.

Configuring CM Offline Control

You can control how long the CMTS tracks offline cable modems, and manage cable modem statistics when a cable modem transitions out of the offline state.

Configuring offline cable modems involves:

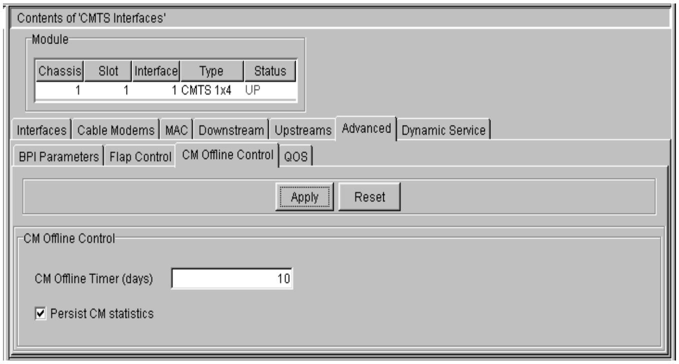
- Specifying the number of days that you want the CMTS to track offline cable modems.
- Specifying whether you want the CMTS to maintain cable modem statistics when the cable modem transitions out of offline state.

To configure CM Offline Control, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **Interfaces.**
2. Click the **Interfaces** tab. Select the interface that you want to configure.
3. Click the **Advanced** tab.
4. Click the **CM Offline Control** tab. The CM Offline Control window appears.
5. Enter values for the parameters. Refer to
6. Click **Apply** to commit the values; or, click **Reset** to return to the default values.

What You See

Figure 18-20 CM Offline Control Window



Contents of 'CMTS Interfaces'

Module

Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

CM Offline Control

CM Offline Timer (days) 10

☑ Persist CM statistics

Parameter Descriptions

This table describes the parameters that you configure for CM offline control:

Table 18-19 CM Offline Control Window Parameters

Parameter	Description
CM Offline Timer (days)	Specify the duration of time, in days, that you want the CMTS to track offline cable modems. By default, offline time is set to 30 days. Acceptable values are 0 to 365 days.

Parameter	Description
Persist CM statistics	Specify if you want the CMTS to maintain the statistics. The options are: ■ Select this option if you want the CMTS to maintain statistics. ■ Leave this option blank if you do not want the CMTS to maintain statistics.

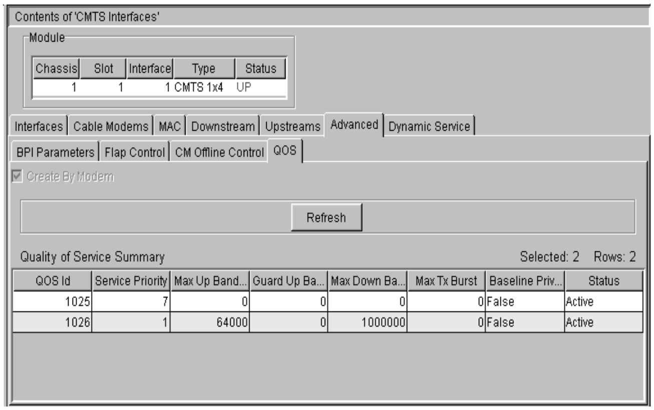
Viewing QoS Profile Summaries

You may view a summary of current QoS Profiles; follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **Interfaces.**
2. Click the **Interfaces** tab. Select the interface that you want to configure.
3. Click the **Advanced** tab.
4. Click the **QoS** tab. The Quality of Service Summary window appears. Refer to Table 18-20.

What You See

Figure 18-21 Quality of Service Summary Window



Contents of 'CMTS Interfaces'

Module

Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

Quality of Service Summary   Selected: 2   Rows: 2

QOS Id	Service Priority	Max Up Band...	Guard Up Ba...	Max Down Ba...	Max Tx Burst	Baseline Priv...	Status
1025	7	0	0	0	0	False	Active
1026	1	64000	0	1000000	0	False	Active

Parameter Descriptions

This table describes the parameters in the Quality of Service Summary window.

Table 18-20 Quality of Service Summary Window Parameters

Parameter	Description
QOS Id	The ID that is dynamically assigned to the profile, to use as a reference to the profile.
Service Priority	Relative priority assigned to this service when allocating bandwidth. Zero indicates lowest priority, and seven indicates the highest priority.
Maximum Upstream Bandwidth	Maximum upstream bandwidth, in bps, the service allows with this service class.
Guaranteed Upstream Bandwidth	Read only. Minimum guaranteed upstream bandwidth, in bps, the service allows with this service class.
Maximum Down Bandwidth	Read only. Maximum downstream bandwidth, in bps, the service allows with this service class.
Max Tx Burst	Read only. Maximum number of mini-slots that may be requested for a single upstream transmission. A value of zero indicates no limit.
Baseline Privacy	Read only. Indicates whether Baseline Privacy is enabled for this service class.
Status	Creates or deletes rows in the table. You must not change a row while it is active.

Viewing Dynamic Services Statistics

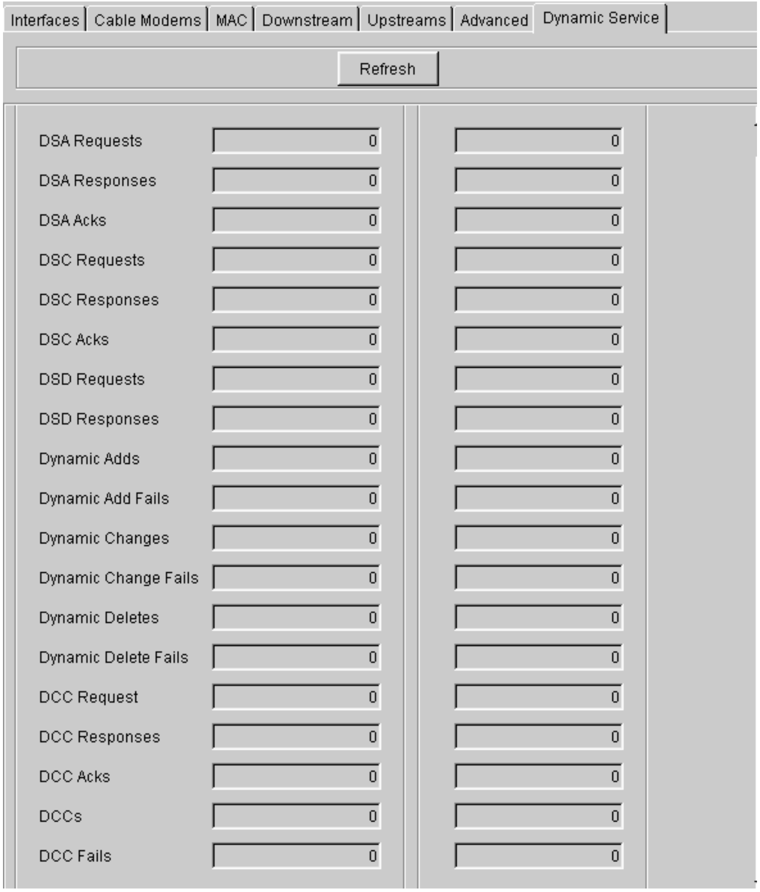
You may view the service flow statistics created through a Dynamic Service, initiated by the cable modem or CMTS.

To view dynamic services statistics, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **CMTS** > **Interfaces.**
2. In the **Interfaces** tab, select the interface you that you wish to view.
3. Click the **Dynamic Service** tab. The **Dynamic Service** window appears.
4. Click **Refresh** to update the information.

What You See

Figure 18-22 Dynamic Service Window. *Note that the left panel displays statistics for the upstream channels, and the right panel displays statistics for the downstream.*



DSA Requests	0	0
DSA Responses	0	0
DSA Acks	0	0
DSC Requests	0	0
DSC Responses	0	0
DSC Acks	0	0
DSD Requests	0	0
DSD Responses	0	0
Dynamic Adds	0	0
Dynamic Add Fails	0	0
Dynamic Changes	0	0
Dynamic Change Fails	0	0
Dynamic Deletes	0	0
Dynamic Delete Fails	0	0
DCC Request	0	0
DCC Responses	0	0
DCC Acks	0	0
DCCs	0	0
DCC Fails	0	0

Parameter Descriptions

This table provides a description of the **Dynamic Service** window

Table 18-21 Dynamic Service Window Parameters.

Parameter	Description
DSA Requests	Number of dynamic service addition requests.
DSA Responses	Number of dynamic service addition responses.

Parameter	Description
DSA Acks	Number of dynamic service addition acknowledgments.
DSC Requests	Number of dynamic service change requests.
DSC Responses	Number of dynamic service change responses.
DSC Acks	Number of dynamic service change acknowledgements.
DSD Requests	Number of dynamic service delete requests.
DSD Responses	Number of dynamic service delete responses.
Dynamic Adds	Number of successful dynamic service addition transactions.
Dynamic Add Fails	Number of failed dynamic service addition transactions.
Dynamic Changes	Number of successful dynamic service change transactions.
Dynamic Change Fails	Number of failed dynamic service change transactions.
Dynamic Deletes	Number of successful dynamic service delete transactions.
Dynamic Delete Fails	Number of failed dynamic service delete transactions.
DCC Requests	Number of dynamic channel change request messages traversing an interface. This value is only non-zero for the downstream.
DCC Responses	Number of dynamic channel change response messages traversing an interface. This value is only non-zero for the upstream.
DCC Acks	Number of dynamic channel change acknowledgements.
DCCs	Number of successful dynamic channel change transactions. This value is only non-zero for the downstream.
DCC Fails	Number of failed dynamic service change transactions. The value is only non-zero for the downstream.

Configuring Modulation Profiles

Modulation profiles contain the profile properties of the CMTS upstream data stream channels. The CMTS supports two profiles for the four upstream channels. Each profile consists of a burst description for the Interval Usage Codes listed below.

Two modulation profiles are configured at the ADC plant and shipped with the Cuda 12000. For the purpose of module profile security, the default profiles may not be modified or deleted.

NOTE: Profiles affect the physical layer. Changes to profile properties affect the performance and function of the CMTS. It is recommended that an expert-level user perform Modulation Profile configuration.

Before You Begin

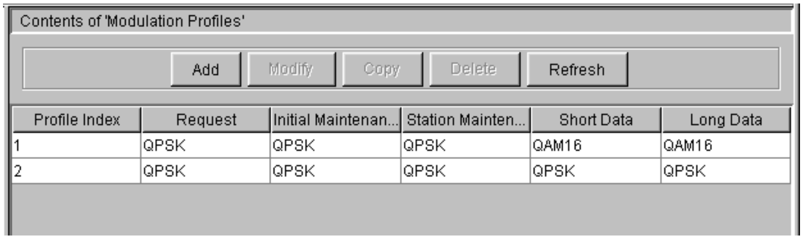
Before you configure modulation profiles, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **CMTS** > **Modulation Profiles.**

The Modulation Profiles window appears. Refer to Table 18-22 for table information.

What You See

Figure 18-23 Modulation Profiles Window



Profile Index	Request	Initial Maintenan...	Station Mainten...	Short Data	Long Data
1	QPSK	QPSK	QPSK	QAM16	QAM16
2	QPSK	QPSK	QPSK	QPSK	QPSK

Parameter Descriptions

This table provides a description of the Modulation Profiles window.

Table 18-22 Modulation Profiles Window Parameters

Parameter	Description
Profile Index	Dynamically assigned number for each profile.
Request	Interval when a request on bandwidth can be sent by the modem.
Initial Maintenance	Interval when new modems can start establishing a connection with CMTS with Initial Ranging Requests.
Station Maintenance	Interval when modems perform periodic ranging for adjusting power, timing and frequency.
Short Data	Interval when a modem can send upstream PDU, which is less than one maximum burst size.
Long Data	Interval when the modem can send upstream PDU, when one burst size exceeds one maximum burst size on the short data interval.

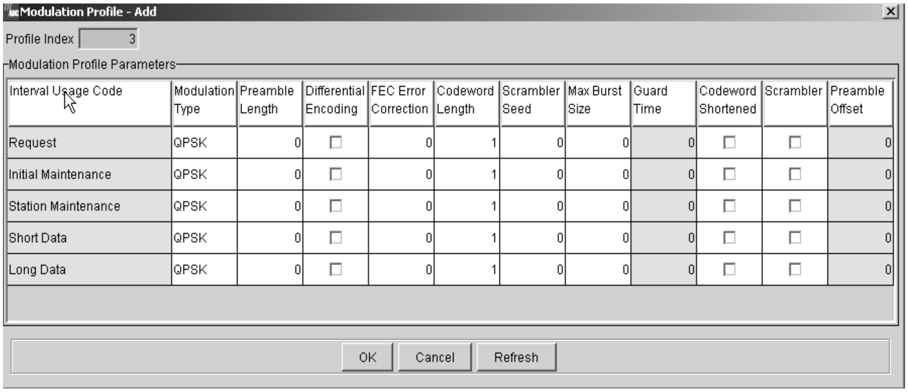
Adding a Modulation Profile

To add a modulation profile, follow this procedure:

1. In the **Modulation Profiles** window, click **Add.** The Modulation Profile - Add window appears, containing a two-dimensional display.
2. Enter values for the parameters. Refer to Table 18-23.
3. Click **Ok** to commit the information or click **Cancel** to exit without saving.

What You See

Figure 18-24 Modulation Profile - Add Window



Modulation Profile - Add

Profile Index 3

Modulation Profile Parameters

Interval Usage Code	Modulation Type	Preamble Length	Differential Encoding	FEC Error Correction	Codeword Length	Scrambler Seed	Max Burst Size	Guard Time	Codeword Shortened	Scrambler	Preamble Offset
Request	QPSK	0	□	0	1	0	0	0	□	□	0
Initial Maintenance	QPSK	0	□	0	1	0	0	0	□	□	0
Station Maintenance	QPSK	0	□	0	1	0	0	0	□	□	0
Short Data	QPSK	0	□	0	1	0	0	0	□	□	0
Long Data	QPSK	0	□	0	1	0	0	0	□	□	0

Parameter Descriptions

This table provides a description of the Modulation Profile - Add window

Table 18-23 Modulation Profile Configuration Parameters.

Parameter	Description
Modulation Type	Sets the modulation type for an upstream port. Choose a value from the pull-down menu. Acceptable values are QPSK and QAM16.
Preamble Length	Specify the preamble pattern length from 2 to 448 bits.
Differential Encoding	Differential Encoding should be enabled when FEC is not used and disabled when FEC is used.
FEC Error Correction	Specify the number of errored bytes that can be corrected ‘in forward error correction code. By default, FEC Error Correction is set at zero. The value of zero indicates no correction is employed. Acceptable values are 0 to 10. The number of check bytes appended will be twice the value that is set.
Codeword Length	Number of data bytes (k) in the forward error correction codeword. Acceptable values are 1 to 255. Note: This parameter is not used if FEC Error Correction is zero.
Scrambler Seed	15 bit seed value for the scrambler polynomial. By default, Scrambler Seed is set to 338.

Parameter	Description
Max Burst Size	Displays the maximum number of mini-slots that can be transmitted during a channel's burst time. A value of zero is transmitted if the burst length is bounded by the allocation MAP rather than this profile. By default, Max Burst Size is set to 0 for all interval usage codes.
Guard Time	Read only. The number of symbol-times that must follow the end of this channel's burst. Guard Time is automatically set based on the Interval Usage Code.
Codeword Shortened	Check this check box in order to enable the truncation of FEC codeword. This field is enabled by default.
Scrambler	Check this check box in order to enable the scrambler. This field is disabled by default.
Preamble Offset	Read-only. Displays the offset into preamble where value bits, or pattern, begins.

Modifying a Profile

For modulation profile security, the first two profiles are default profiles that are shipped with the Cuda 12000 and may not be modified. Only profiles that have been added by the network administrator at your cable plant may be modified.

To copy a modulation profile, follow this procedure:

1. In the Modulation Profiles window, select the row that includes the Profile Index number you wish to change.
2. Click **Modify**. The Modulation Profile - Modify window appears.
3. Update information as necessary. Refer to Table 18-23.
4. Click **Ok** to commit the information or click **Cancel** to exit without saving.

Deleting a Profile

A profile can be deleted only if it is not being referred by any of the upstream channels. To delete a modulation profile, follow this procedure:

1. In the Modulation Profiles window, select the row that includes the Profile Index number you wish to change.
2. Click **Delete**. The profile immediately deletes from the CMTS application module. There is no Reset option. If you wish to retrieve the deleted profile, you must reboot the CMTS module, using the Reset button on the module.
   - *Note: You can only retrieve a profile if you did not Save after you deleted the profile.*

Copying a Modulation Profile

The Cuda 12000 allows you to copy a module profile to use as a template. All existing profiles may be copied, including the default profiles. The new profile, which is created by the template, may be modified as necessary for your environment.

To copy existing modulation profiles, follow this procedure:

1. In the Modulation Profiles window, select the row that includes the Profile you wish to copy.
2. Click **Copy**. The Copy Profile Index "n" window appears, where "n" represents the index number you are copying.
3. Update information as necessary. Refer to Table 18-23.
4. Click **Ok** to commit the information or click **Cancel** to exit without saving.

19 CONFIGURING BPI PLUS CERTIFICATES

This chapter describes how to configure DOCSIS 1.1 BPI+ certificates. Cuda 12000 BPI+ certificate configuration conforms with *Data-Over-Service Interface Specifications*: *Radio Frequency Interface Specification*, SP-RFLv1.1-106-001215.

DOCSIS 1.1 BPI+ provides additional secure authentication of cable modems through digital certificates. A cable modem can use a digital signature to verify that the software image that it downloaded was not altered or corrupted in transit.

For a BPI+ exchange between the cable modem termination system (CMTS) and a cable modem, you must configure two types of digital certificates, which are:

- **Manufacturer/CA Certificates**. A cable modem sends a Manufacturer/CA Certificate when sending authorization information to the CMTS.
- **CM Certificate**. The CM certificate is required when the cable modem requests authorization.

Access Privileges

Prerequisites

BPI+ is the final stage in initializing cable modems for communication with the CMTS. Before you can configure BPI+, the cable modem must have been initialized as follows:

- Provisioned with BPI+ enabled (Refer to the *FastFlow Broadband Provisioning Manager GUI-based Administration Guide, or the documentation of your external provisioning manager*);
- Registered with the CMTS;
- Configured for BPI+ Privacy Authorization and Privacy TEK;
- Configured for Privacy Multicast with IGMP protocol.

Configuring Manufacturer/CA Certificates

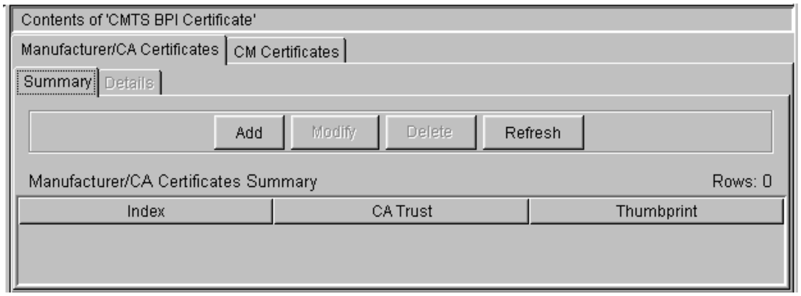
A Certificate Authority (CA) is a self-signed certificate containing the DOCSIS CAs trusted public key. The manufacturer issues an X.509 certificate that binds the cable modem public key to other identifying information.

To configure Manufacturer/CA Certifications, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **CMTS** > **BPI Certificate**
2. Click the **Manufacturer/CA Certificates** tab**.**
3. Click **Refresh.**

The Manufacturer/CA Certificates window appears with the Summary tab clicked by default (Figure 19-1, "Manufacturer/CA Certificates Summary window." Click Refresh to update the window.

Figure 19-1 Manufacturer/CA Certificates Summary window.



Contents of 'CMTS BPI Certificate'

Manufacturer/CA Certificates Summary   Rows: 0

Index	CA Trust	Thumbprint

Adding a CA Certificate

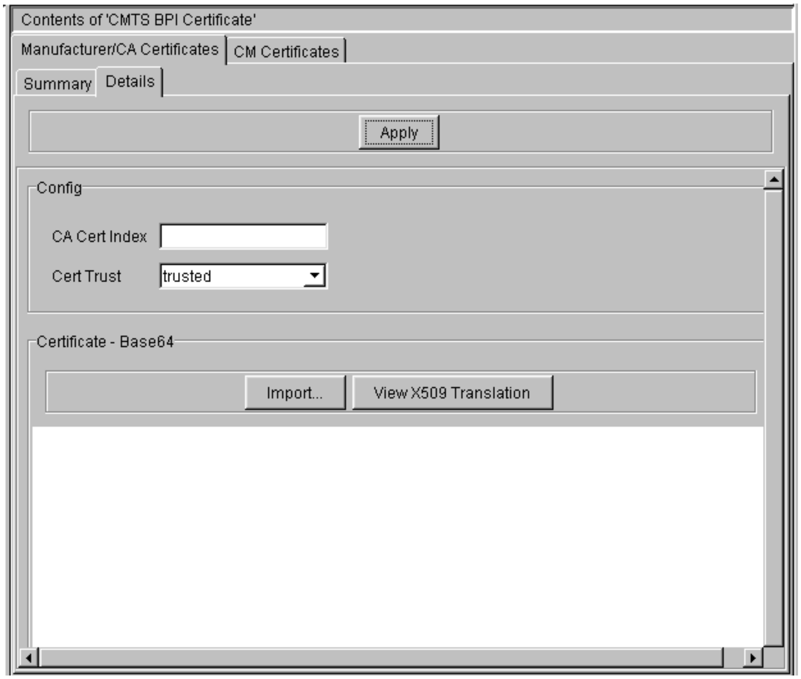
To add a CA certificate, follow this procedure:

1. From the **Summary** window, click **Add**. The Details window appears.
2. Enter values for the parameters. Refer to Table 19-1.
3. Click the **Import** button to import a certification file from the server. The **Select a certificate file** window appears (Figure 19-8, "Select a Manufacturer/CA Certificate File Window").
4. Navigate through the file structure and select the desired file. Prerequisites:
   - You must have already created the directory structure;

- The file must be in 64 base format.

5. Click **Contents** to get the file’s contents. The results of importing appears in Figure 19-4, “After Importing Manufacturer/CA Certificate File Contents”. Or, you can click **Cancel** to return to the previous window.
6. Click **Apply** to commit the information.

Figure 19-2 Manufacturer/CA Certificates Details Window



CA Cert Index

Cert Trust: trusted

Parameter Descriptions

This table describes the parameters of the Details window.

Table 19-1 Manufacturer/CA Certificates Detail Parameters

Parameter	Description
CA Cert Index	Specifies an index number for the manufacturer CA certificate. Values range from 1 to 10000.
Cert Trust	Specifies one of the following levels of trust. (For more information on levels of trust, refer to the *DOCSIS Baseline Privacy Plus Interface Specification*.)

Parameter	Description
	■ trusted - Specifies that the certificate is trusted. Trusted certificates are valid certificates. ■ untrusted - Specifies that the certificate is untrusted. Untrusted certificates are invalid certificates. ■ chained - Specifies that the certificate's level of trust is chained. ■ root - Specifies that the certificate's level of trust is root. Only the DOCSIS Root CA Certificate (a self-signed certificate containing the DOCSIS Root CA's trusted public key) must be marked as Root. However, a CMTS may support multiple Root CA Certificates. At least one root certificate must be provisioned.

Figure 19-3 Select a Manufacturer/CA Certificate File Window

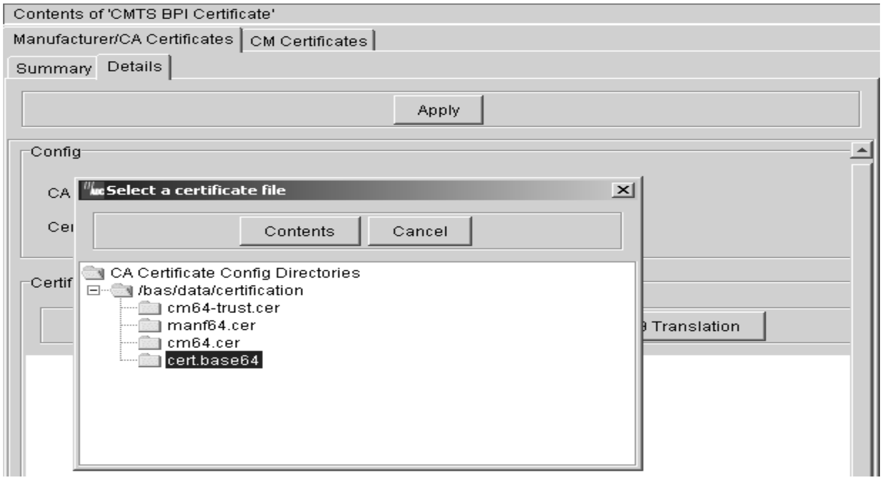
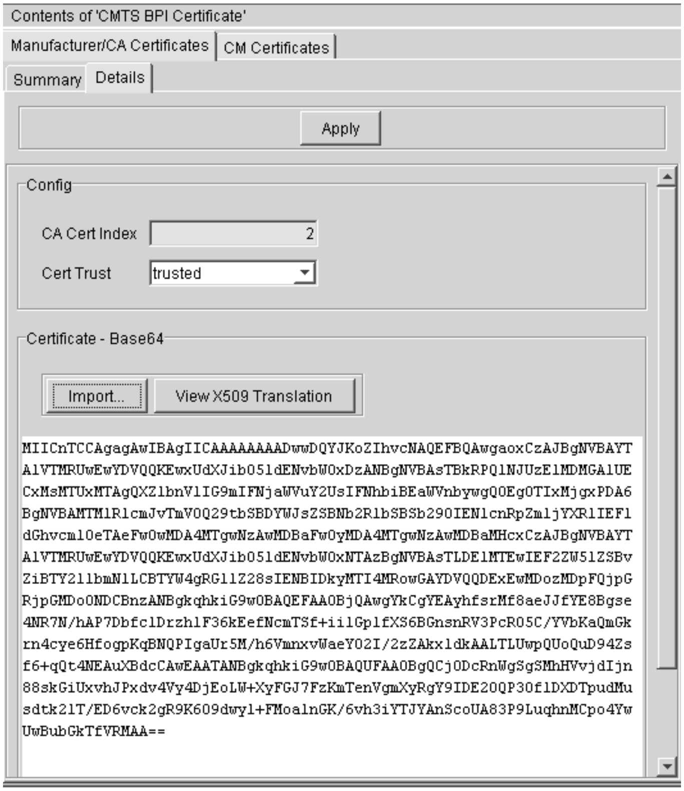


Figure 19-4 After Importing Manufacturer/CA Certificate File Contents



Contents of 'CMTS BPI Certificate'

Config

CA Cert Index: 2

Cert Trust: trusted

Certificate - Base64

```
MIICnTCCAgagAwIBAgIICAAAAAAAADwwDQYJKoZIhvcNAQEFBQAwgaoxCzAJBgNVBAYT
AlVTMRUwEwYDVQQKEwxUdXJib05ldENvbW0xDzANBgNVBAsTBkRPQ1NJUzElMDMGA1UE
CxMsMTUxMTAgQXZlbnVlIG9mIFNjaWVuY2UsIFNhbiBEaWVnbywgQ0EgOTIxMjgxPDA6
BgNVBAMTM1RlcmJvTmV0Q29tbSBDYWJsZSBNb2RlbSBSb290IENlcnRpZmljYXRlIEF1
dGhvcml0eTAeFw0wMDA4MTgwNzAwMDBaFw0yMDA4MTgwNzAwMDBaMHcxCzAJBgNVBAYT
AlVTMRUwEwYDVQQKEwxUdXJib05ldENvbW0xNTAzBgNVBAsTLDE1MTEwIEF2ZW51ZSBv
ZiBTY2llbmNlLCBTYW4gRGllZ28sIENBIDkyMTI4MRowGAYDVQQDExEwMDozMDpFQjpG
RjpGMDo0NDCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAyhfsrMf8aeJJfYE8Bgse
4NR7N/hAP7DbfclDrzhlF36kEefNcmTSf+iilGplfXS6BGnsnRV3PcR05C/YVbKaQmGk
rn4cye6HfogpKqBNQPIgaUr5M/h6VmnxvWaeY02I/2zZAkxldkAALTLUwpQUoQuD94Zs
f6+qQt4NEAuXBdcCAwEAATANBgkqhkiG9w0BAQUFAAOBgQCj0DcRnWgSgSMhHVvjdIjn
88skGiUxvhJPxdv4Vy4DjEoLW+XyFGJ7FzKmTenVgmXyRgY9IDE20QP30flDXDTpudMu
sdtk2lT/ED6vck2gR9K609dwyl+FMoalnGK/6vh3iYTJYAnScoUA83P9LuqhnMCpo4Yw
UwBubGkTfVRMAA==
```

Modifying a CA Certificate

To modify a CA certificate, follow this procedure:

1. From the **Summary** window, select the CA certificate you wish to modify.
2. Click **Modify**. The Details window appears (Figure 19-2,“Manufacturer/CA Certificates Details Window”).
3. Update with the necessary information.
4. Click the **Import** button to import an updated certification file from the server. The Select a Certificate File window appears.
5. Navigate through the file structure to the import file location.

6. Click **Contents** to import the file or click **Cancel** to return to the previous screen.
7. Click **Apply** to commit the information.
8. Click **Refresh** to update the information.

Deleting a CA Certificate

To delete a CA certificate, follow this procedure:

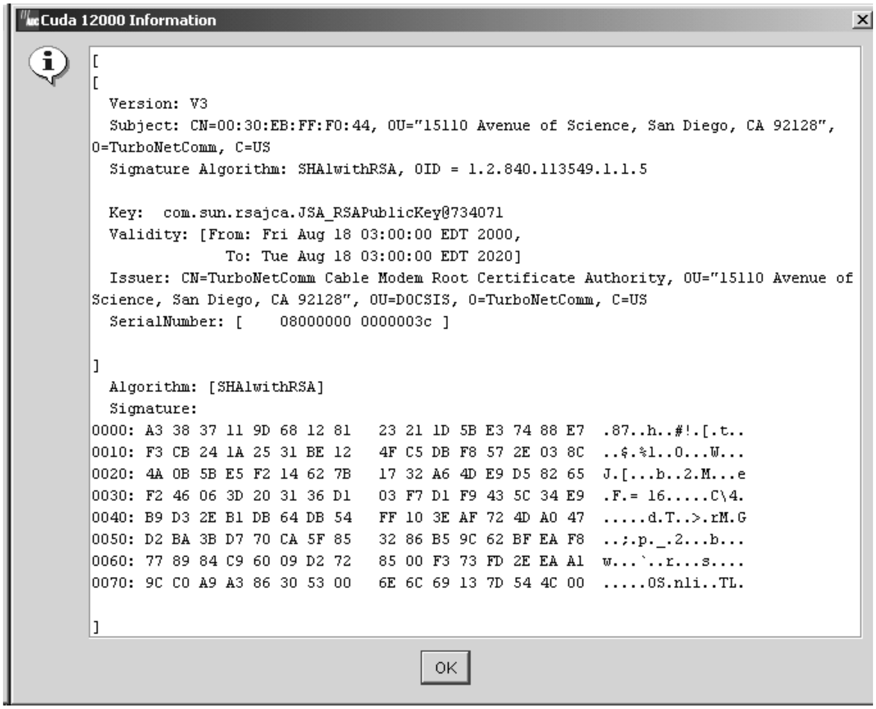
1. From the **Summary** window, select the CA certificate you wish to delete.
2. Click **Delete**. A confirmation window appears
3. Click **Ok** to continue or click **Cancel** to cancel the deletion.
4. Click **Refresh** to update the window.

Viewing a X509 Certificate

BPI+ uses the X.509 digital certificate to authenticate key exchanges between the cable modem and CMTS. To view the X509 certificate, follow this procedure:

1. From the **Summary** window, select the CA certificate that you wish to view.
2. Click the **View X509 Translation** tab. The certificate information appears.

Figure 19-5 CA X509 Certificate Details Window



```
[
[
  Version: V3
  Subject: CN=00:30:EB:FF:F0:44, OU="15110 Avenue of Science, San Diego, CA 92128",
O=TurboNetComm, C=US
  Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5

  Key:  com.sun.rsajca.JSA_RSAPublicKey@734071
  Validity: [From: Fri Aug 18 03:00:00 EDT 2000,
               To: Tue Aug 18 03:00:00 EDT 2020]
  Issuer: CN=TurboNetComm Cable Modem Root Certificate Authority, OU="15110 Avenue of
Science, San Diego, CA 92128", OU=DOCSIS, O=TurboNetComm, C=US
  SerialNumber: [    08000000 0000003c ]

]
  Algorithm: [SHA1withRSA]
  Signature:
0000: A3 38 37 11 9D 68 12 81   23 21 1D 5B E3 74 88 E7  .87..h..#!.[.t..
0010: F3 CB 24 1A 25 31 BE 12   4F C5 DB F8 57 2E 03 8C  ..$.%1..O...W...
0020: 4A 0B 5B E5 F2 14 62 7B   17 32 A6 4D E9 D5 82 65  J.[...b..2.M...e
0030: F2 46 06 3D 20 31 36 D1   03 F7 D1 F9 43 5C 34 E9  .F.= 16.....C\4.
0040: B9 D3 2E B1 DB 64 DB 54   FF 10 3E AF 72 4D A0 47  .....d.T..>.rM.G
0050: D2 BA 3B D7 70 CA 5F 85   32 86 B5 9C 62 BF EA F8  ..;.p._.2...b...
0060: 77 89 84 C9 60 09 D2 72   85 00 F3 73 FD 2E EA A1  w...`..r...s....
0070: 9C C0 A9 A3 86 30 53 00   6E 6C 69 13 7D 54 4C 00  .....0S.nli..TL.

]
```

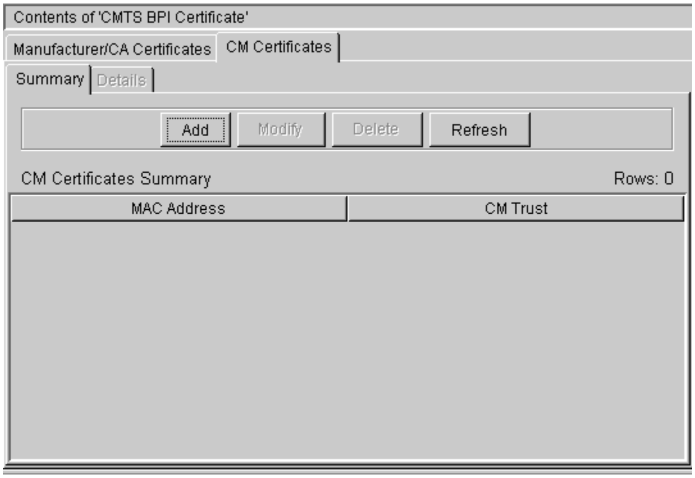
Configuring Cable Modem (CM) Certificates

Cable modem (CM) Certificates are assigned to provisioned cable modems. A CM Certificate is required when the cable modem requests authorization.

You can add, modify, or delete CM Certificates that the CMTS acquired. To configure CM Certificates, follow this procedure:

1. Navigate to **Network Browser >** GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **CMTS** > **BPI Certificate**
2. Click the **CM Certificates** tab**.**
3. Click the **Summary** tab.
4. Click **Refresh** to update the window**.**

Figure 19-6 CM Certificates Summary window.



Adding a CM Certificate

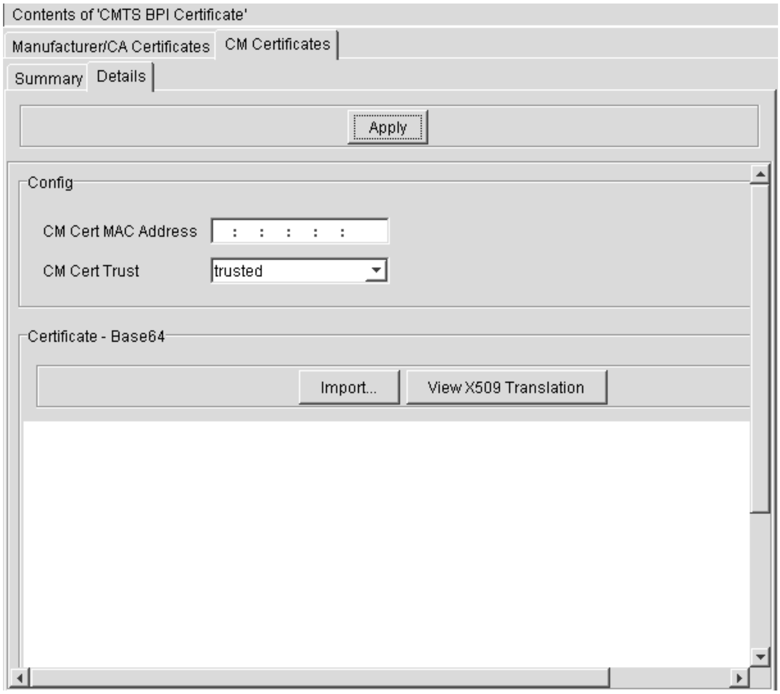
To add a CM Certificate, follow this procedure:

1. From the **Summary** window, click **Add**. The Details window appears.
2. Enter values for the parameters. Refer to Table 19-2.
3. Click the **Import** button to import a certification file from the server. The Select a Certificate File window appears (Figure 19-3, “Select a Manufacturer/CA Certificate File Window”).

4. Navigate through the file structure to the desired file. Prerequisites:
   - You must have already created the directory structure;
   - The file must be in 64 base format, which is a requirement of the user interface.
5. Click **Contents** to get the file's contents. The results of importing appears in Figure 19-4, "After Importing Manufacturer/CA Certificate File Contents". Or, you can click **Cancel** to return to the previous window.
6. Click **Apply** to commit the information.
7. Click **Refresh** to update the window.

What You See

Figure 19-7 CM Certificate Details window



Contents of 'CMTS BPI Certificate'

Config

CM Cert MAC Address : : : : :

CM Cert Trust trusted

Certificate - Base64

Parameter Descriptions

This table describes the parameters of the Details window.

Table 19-2 CM Certificates Detail Parameters

Parameter	Description
CM Cert MAC Address	The MAC address of the cable modem for which you want to display certificates.
CM Cert Trust	Specifies one of the following levels of trust. (For more information on levels of trust, refer to the *DOCSIS Baseline Privacy Plus Interface Specification*.) ■ trusted - Specifies that the certificate is trusted. Trusted certificates are valid certificates. ■ untrusted - Specifies that the certificate is untrusted. Untrusted certificates are invalid certificates.

Figure 19-8 Select a Certificate File Window

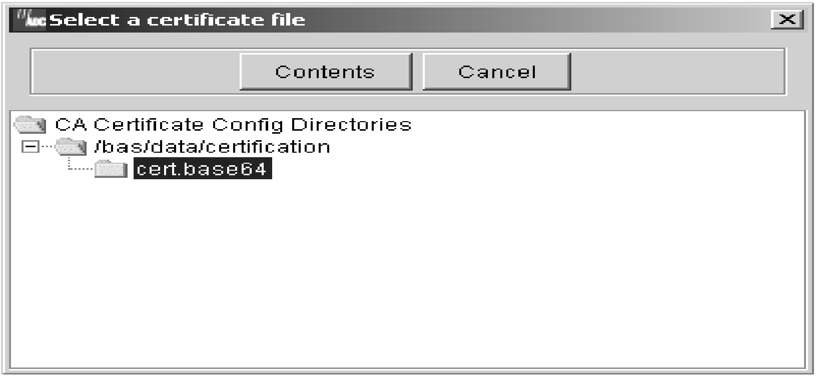
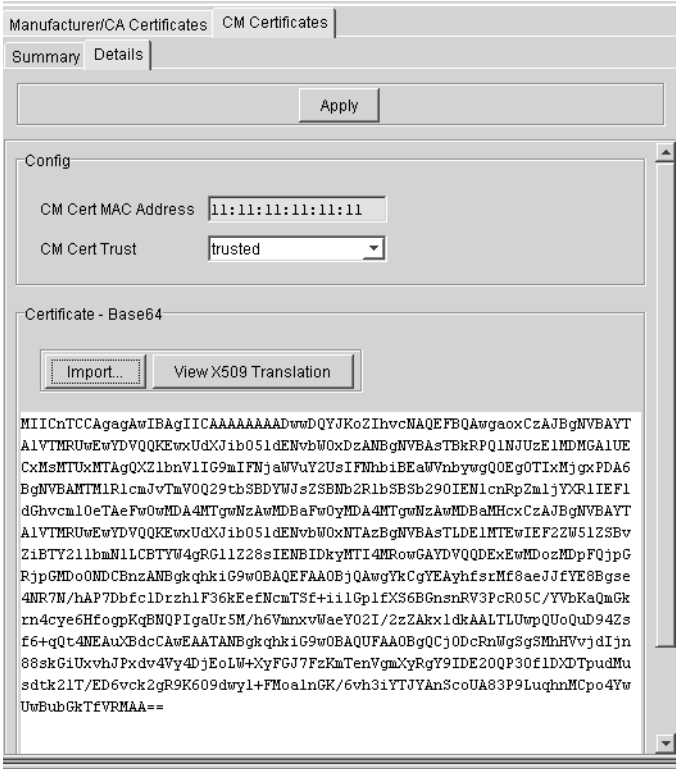


Figure 19-9 Results of Importing a CM Certificate File



CM Cert MAC Address 11:11:11:11:11:11

CM Cert Trust trusted

```
MIICnTCCAgagAwIBAgIICAAAAAAAADwwDQYJKoZIhvcNAQEFBQAwgaoxCzAJBgNVBAYT
AlVTMRUwEwYDVQQKEwxUdXJib05ldENvbW0xDzANBgNVBAsTBkRPQ1NJUzElMDMGA1UE
CxMsMTUxMTAgQXZlbnVlIG9mIFNjaWVuY2UsIFNhbiBEaWVnbywgQ0EgOTIxMjgxPDA6
BgNVBAMTMlRlcmJvTmV0Q29tbSBDYWJsZSBNb2RlbSBSb290IENlcnRpZmljYXRlIEFl
dGhvcml0eTAeFw0wMDA4MTgwNzAwMDBaFw0yMDA4MTgwNzAwMDBaMHcxCzAJBgNVBAYT
AlVTMRUwEwYDVQQKEwxUdXJib05ldENvbW0xNTAzBgNVBAsTLDElMTEwIEF2ZW5lZSBv
ZiBTY2llbmNlLCBTYW4gRGllZ28sIENBIDkyMTI4MRowGAYDVQQDExEwMDozMDpFQjpG
RjpGMDo0NDCBnzANBgkqhkiG9w0BAQEFAA0BjQAwgYkCgYEAyhfsrMf8aeJJfYE8Bgse
4NR7N/hAP7DbfclDrzhlF36kEefNcmTSf+iilGplfXS6BGnsnRV3PcR05C/YVbKaQmGk
rn4cye6HfogpKqBNQPIgaUr5M/h6VmnxvWaeY02I/2zZAkxldkAALTLUwpQUoQuD94Zs
f6+qQt4NEAuXBdcCAwEAATANBgkqhkiG9w0BAQUFAA0BgQCj0DcRnWgSgSMhHVvjdIjn
88skGiUxvhJPxdv4Vy4DjEoLW+XyFGJ7FzKmTenVgmXyRgY9IDE20QP30flDXDTpudMu
sdtk2lT/ED6vck2gR9K609dwyl+FMoalnGK/6vh3iYTJYAnScoUA83P9LuqhnMCpo4Yw
UwBubGkTfVRMAA==
```

Modifying a CM Certificate

To modify a cable modem certificate, follow this procedure:

1. From the **Summary** window, select the cable modem certificate you wish to modify.
2. Click **Modify**. The Details window appears (Figure 19-7,"CM Certificate Details window").
3. Update the necessary information. Refer to Table 19-2.
4. To import an updated file from a server, click the **Import** button. The Select a Certificate File window appears.
5. Navigate through the file structure to the import file location.
6. Click **Contents** to import the file or click **Cancel**.

7. Click **Apply** to commit the changes.
8. Click **Refresh** to update the information.

Deleting a CM Certificate

To delete a cable modem certificate, follow this procedure:

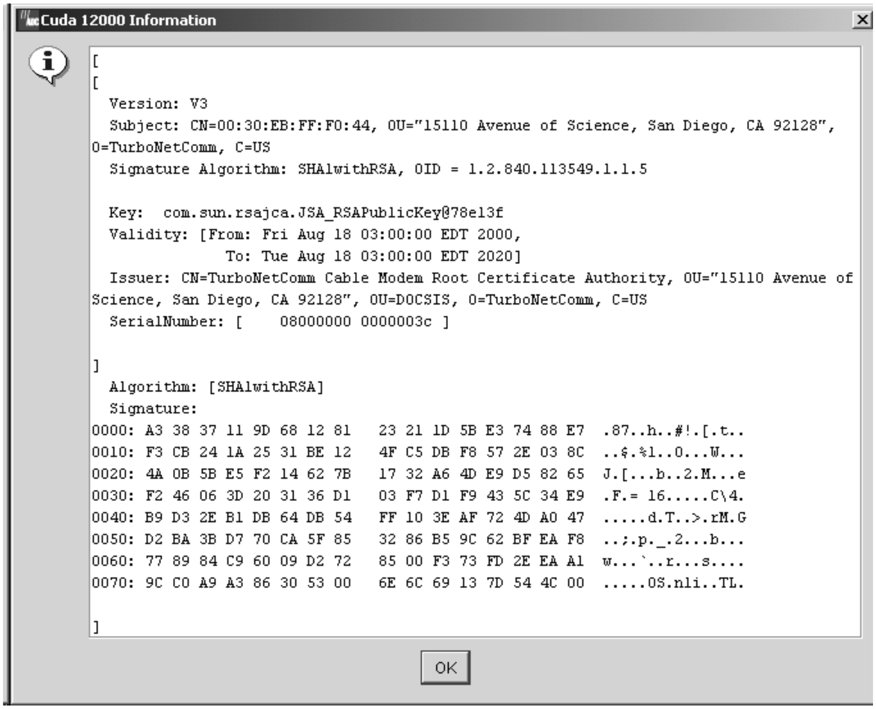
1. From the **Summary** window, select the cable modem certificate you wish to delete.
2. Click **Delete**. A confirmation window appears
3. Click **Ok** to continue or click **Cancel** to cancel the deletion.
4. Click **Refresh** to update the information.

Viewing a X509 Certificate

BPI+ uses the X.509 digital certificate to authenticate key exchanges between the cable modem and CMTS. To view the X509 certificate, follow this procedure:

1. From the **Summary** window, select the CM certificate that you wish to view.
2. Click the **View X509 Translation** tab. The certificate information appears.

Figure 19-10 X509 CM Certificate Details Window



```
[
[
  Version: V3
  Subject: CN=00:30:EB:FF:F0:44, OU="15110 Avenue of Science, San Diego, CA 92128",
O=TurboNetComm, C=US
  Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5

  Key:  com.sun.rsajca.JSA_RSAPublicKey@78e13f
  Validity: [From: Fri Aug 18 03:00:00 EDT 2000,
               To: Tue Aug 18 03:00:00 EDT 2020]
  Issuer: CN=TurboNetComm Cable Modem Root Certificate Authority, OU="15110 Avenue of
Science, San Diego, CA 92128", OU=DOCSIS, O=TurboNetComm, C=US
  SerialNumber: [    08000000 0000003c ]

]
  Algorithm: [SHA1withRSA]
  Signature:
0000: A3 38 37 11 9D 68 12 81   23 21 1D 5B E3 74 88 E7  .87..h..#!.[.t..
0010: F3 CB 24 1A 25 31 BE 12   4F C5 DB F8 57 2E 03 8C  ..$.%1..O...W...
0020: 4A 0B 5B E5 F2 14 62 7B   17 32 A6 4D E9 D5 82 65  J.[...b..2.M...e
0030: F2 46 06 3D 20 31 36 D1   03 F7 D1 F9 43 5C 34 E9  .F.= 16.....C\4.
0040: B9 D3 2E B1 DB 64 DB 54   FF 10 3E AF 72 4D A0 47  .....d.T..>.rM.G
0050: D2 BA 3B D7 70 CA 5F 85   32 86 B5 9C 62 BF EA F8  ..;.p._.2...b...
0060: 77 89 84 C9 60 09 D2 72   85 00 F3 73 FD 2E EA A1  w...`..r...s....
0070: 9C C0 A9 A3 86 30 53 00   6E 6C 69 13 7D 54 4C 00  .....0S.nli..TL.

]
```

20 MANAGING CABLE MODEMS

The purpose of cable modem management is to monitor and manage cable modem activity on the network. The Cuda 12000 provides the ability to monitor activity for an interface or on a per cable modem basis. Monitoring and managing cable modem activity on the Cuda 12000 includes the following functions:

- Managing Status Summary
- Viewing Cable Modem Statistics
- Monitoring Cable Modem Services Information
- Managing BPI Parameters
- Monitoring the Flap List
- Monitoring Quality of Service

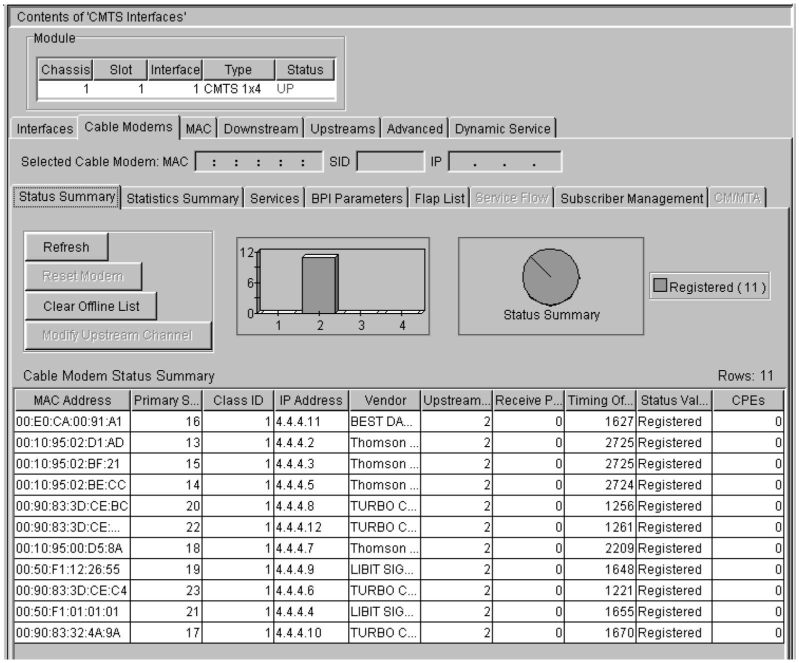
Before You Begin

Before you begin, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName **Configuration** > **CMTS** > **Interfaces.**
2. Click the **Interfaces** tab. The CMTS Interface Summary window appears.
3. Select the CMTS interface that you wish to manage.
4. Click the **Cable Modems** tab. The Cable Modems window appears.

What You See

Figure 20-1 Cable Modem Window



Contents of 'CMTS Interfaces'

Module

Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

Selected Cable Modem: MAC : : : : : SID IP . . .

Cable Modem Status Summary Rows: 11

MAC Address	Primary S...	Class ID	IP Address	Vendor	Upstream...	Receive P...	Timing Of...	Status Val...	CPEs
00:E0:CA:00:91:A1	16	1	4.4.4.11	BEST DA...	2	0	1627	Registered	0
00:10:95:02:D1:AD	13	1	4.4.4.2	Thomson ...	2	0	2725	Registered	0
00:10:95:02:BF:21	15	1	4.4.4.3	Thomson ...	2	0	2725	Registered	0
00:10:95:02:BE:CC	14	1	4.4.4.5	Thomson ...	2	0	2724	Registered	0
00:90:83:3D:CE:BC	20	1	4.4.4.8	TURBO C...	2	0	1256	Registered	0
00:90:83:3D:CE:...	22	1	4.4.4.12	TURBO C...	2	0	1261	Registered	0
00:10:95:00:D5:8A	18	1	4.4.4.7	Thomson ...	2	0	2209	Registered	0
00:50:F1:12:26:55	19	1	4.4.4.9	LIBIT SIG...	2	0	1648	Registered	0
00:90:83:3D:CE:C4	23	1	4.4.4.6	TURBO C...	2	0	1221	Registered	0
00:50:F1:01:01:01	21	1	4.4.4.4	LIBIT SIG...	2	0	1655	Registered	0
00:90:83:32:4A:9A	17	1	4.4.4.10	TURBO C...	2	0	1670	Registered	0

Tab Descriptions

This table provides a description of the tabs in the Cable Modems window.

Table 20-1 Description of Cable Modems Tabs.

Tabs	Description
Status Summary	Manages available cable modems by MAC Address.
Services	Monitors, by Service ID (SID) numbers, the CM Status and QoS Profiles for available cable modems.
BPI Parameters	Manages and monitors the BPI+ for cable modems with data privacy across the Hybrid Fiber-Coaxial (HFC) network by encrypting traffic flows between cable modems and the CMTS.
Flap List	Read-only. Monitors, by MAC Address, the flap activity of a cable modem.

Tabs	Description
Service Flow	Monitors the DOCSIS 1.1 Quality of Service (QoS) activities for cable modems.
CM/MTA	Monitoring cable modem and Multimedia Terminal Adaptors (MTA) activity.
Subscriber Management	Configures filtering criteria for added security for cable modems and CPE devices.

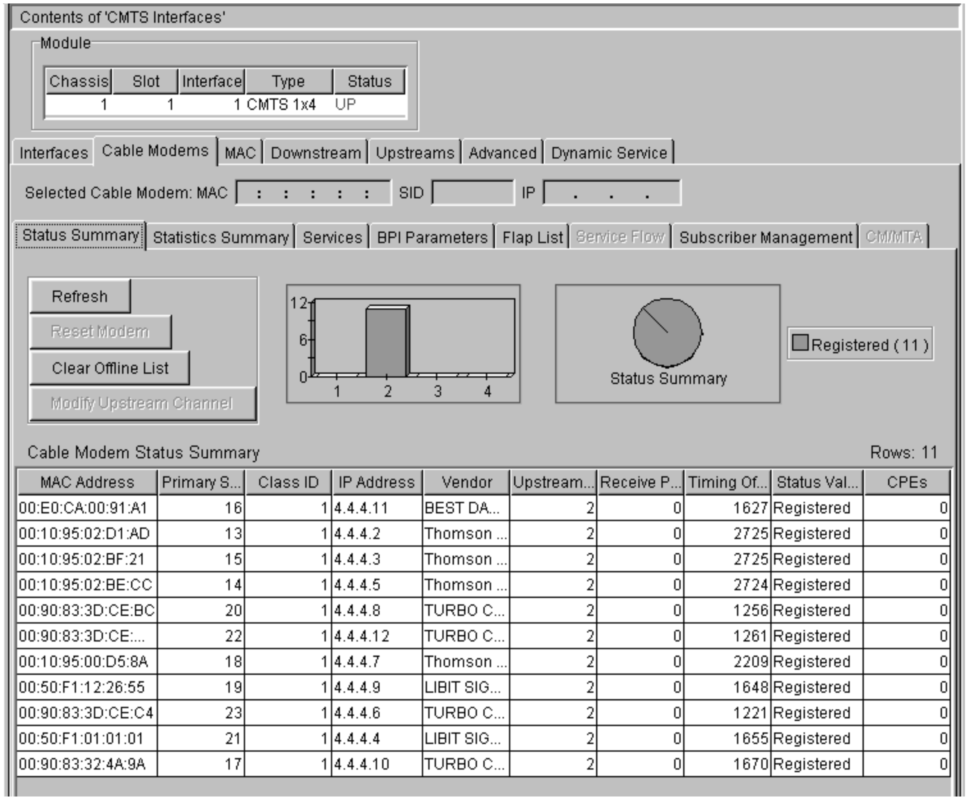
Managing Status Summary

Status Summary functions include resetting cable modems and switching the upstream channels assigned to cable modems. To manage the status functions, follow this procedure:

1. In the Cable Modems window, click the **Status Summary** tab. The Cable Modem Status Summary window appears.
2. Click **Refresh** to update the information.

What You See

Figure 20-2 Status Summary Window



Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

Selected Cable Modem: MAC : : : : : SID IP . . .

Cable Modem Status Summary

Rows: 11

MAC Address	Primary S...	Class ID	IP Address	Vendor	Upstream...	Receive P...	Timing Of...	Status Val...	CPEs
00:E0:CA:00:91:A1	16	1	4.4.4.11	BEST DA...	2	0	1627	Registered	0
00:10:95:02:D1:AD	13	1	4.4.4.2	Thomson ...	2	0	2725	Registered	0
00:10:95:02:BF:21	15	1	4.4.4.3	Thomson ...	2	0	2725	Registered	0
00:10:95:02:BE:CC	14	1	4.4.4.5	Thomson ...	2	0	2724	Registered	0
00:90:83:3D:CE:BC	20	1	4.4.4.8	TURBO C...	2	0	1256	Registered	0
00:90:83:3D:CE:...	22	1	4.4.4.12	TURBO C...	2	0	1261	Registered	0
00:10:95:00:D5:8A	18	1	4.4.4.7	Thomson ...	2	0	2209	Registered	0
00:50:F1:12:26:55	19	1	4.4.4.9	LIBIT SIG...	2	0	1648	Registered	0
00:90:83:3D:CE:C4	23	1	4.4.4.6	TURBO C...	2	0	1221	Registered	0
00:50:F1:01:01:01	21	1	4.4.4.4	LIBIT SIG...	2	0	1655	Registered	0
00:90:83:32:4A:9A	17	1	4.4.4.10	TURBO C...	2	0	1670	Registered	0

The Status Summary window is divided into the following panels:

- Cable Modem Status Summary window

- Buttons
  - Refresh
  - Reset Cable Modem
  - Clear Offline List
  - Modify Upstream Channel
- Graphs of cable modem status
  - Bar chart -- Horizontal axis.
  - Pie chart-- Proportional classification of cable modems by status value.

Parameter Descriptions

This table provides a description of the Status Summary window.

Table 20-2 Status Summary Window Parameters.

Parameter	Description
MAC Address	Cable modem’s unique physical address.
Primary SID	Primary Service ID number assigned dynamically to the cable modem by the CMTS.
Class ID	DOCSIS 1.0 class of service ID.
IP Address	IP Address assigned through DHCP Server configuration. If the cable modem has not completed registration, then the IP address displayed is 0.0.0.0.
Vendor	Identifies the cable modem vendors that were added to the provisioning database.
Upstream Channel	Upstream channel to which this cable modem is assigned.
Receive Power	Receive power level from the CMTS for the upstream interface from the cable modem. By default, the Receive Power is set at 0, which is the optimal setting for the upstream power level. Acceptable values are -160 to 260 TenthdBmV. The Receive Power is dependent on the selected channel-width
Timing Offset	A measure of the current round-trip time for this cable modem. Timing Offset is used for timing cable modem upstream transmissions to ensure synchronized arrivals at the CMTS. Units are in terms of (6.25 microseconds/64). A value of zero is returned if the time is unknown.

Parameter	Description
Status Value	Current cable modem connectivity state specified in the RF Interface Specification. Returned status information is the cable modem status as learned by the CMTS. A detail description of the Status Values is listed below.Current cable modem connectivity state specified in the RF Interface Specification. Returned status information is the cable modem status as learned by the CMTS.
CPEs	The number of CPE devices attached to this cable modem.

Resetting a Cable Modem

To reset a cable modem, follow this procedure:

1. In the Cable Modems window, click the **Status Summary** tab.
2. In the Status Summary window (Figure 20-2), select the row that includes the MAC Address of the cable modem you wish to reset.
3. Click the **Reset Modem** button. The cable modem is immediately removed from the CMTS. This is not a permanent setting, but is valid until the cable modem performs the reboot or power cycle.
4. Click **Refresh** to update the information.

Clearing Offline Cable Modems from Status

You may remove offline cable modems from the status summary list.

To remove offline cable modems, follow this procedure:

1. In the Cable Modems window, click the **Status Summary** tab.
2. In the Status Summary window (Figure 20-2), select the row that includes the offline cable modem you wish to remove.
3. Click the **Clear Offline List** button. This is not a permanent setting, but is valid until the cable modem performs the reboot or power cycle.

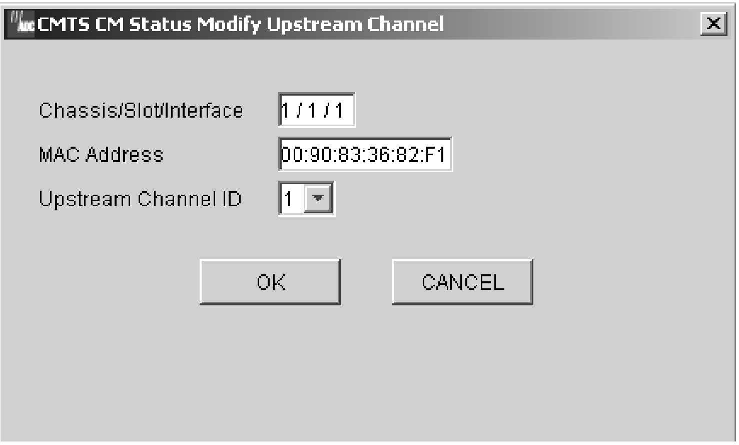
Modifying an Upstream Channel

Modifying an upstream channel switches a cable modem to another Upstream Channel ID. A modem can only be switched to an upstream channel that is Up. To change the Upstream Channel ID follow this procedure:

1. In the Cable Modems window, click the **Status Summary** tab.
2. Select the row that includes the MAC Address of the cable modem you wish to change (Figure 20-2, “Status Summary Window”).
3. Click the **Modify Upstream Channel** button. The CM Status Modify Upstream Channel window appears.
4. From the menu, choose another upstream channel ID.
5. Choose **Ok** to apply the changes or click **Cancel** to exit without saving.
6. Click Refresh to update the information.

What You See

Figure 20-3 CM Status Modify Upstream Channel Window



CMTS CM Status Modify Upstream Channel

Chassis/Slot/Interface 1 / 1 / 1

MAC Address 00:90:83:36:82:F1

Upstream Channel ID 1

Viewing Cable Modem Statistics

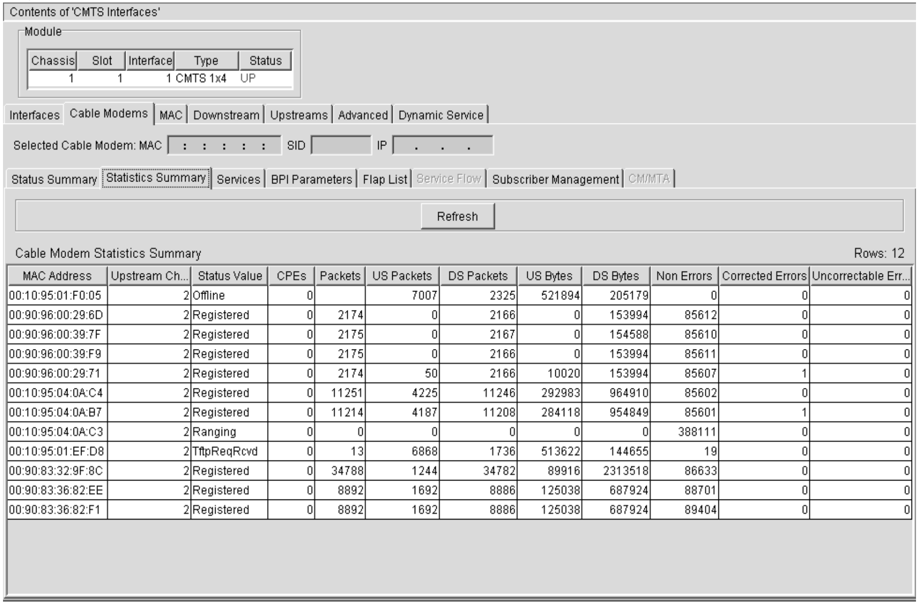
You may view statistics of the cable modems for a specific interface.

To view cable modem statistics, follow this procedure:

1. In the Cable Modems window, click the **Statistics Summary** tab. The Cable Modem Statistics Summary window appears.
2. Click **Refresh** to update the information.

What You See

Figure 20-4 Cable Modem Statistics Summary Window



Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

Cable Modem Statistics Summary

MAC Address	Upstream Ch...	Status Value	CPEs	Packets	US Packets	DS Packets	US Bytes	DS Bytes	Non Errors	Corrected Errors	Uncorrectable Err...
00:10:95:01:F0:05	2	Offline	0		7007	2325	521894	205179	0	0	0
00:90:96:00:29:6D	2	Registered	0	2174	0	2166	0	153994	85612	0	0
00:90:96:00:39:7F	2	Registered	0	2175	0	2167	0	154588	85610	0	0
00:90:96:00:39:F9	2	Registered	0	2175	0	2166	0	153994	85611	0	0
00:90:96:00:29:71	2	Registered	0	2174	50	2166	10020	153994	85607	1	0
00:10:95:04:0A:C4	2	Registered	0	11251	4225	11246	292983	964910	85602	0	0
00:10:95:04:0A:B7	2	Registered	0	11214	4187	11208	284118	954849	85601	1	0
00:10:95:04:0A:C3	2	Ranging	0	0	0	0	0	0	388111	0	0
00:10:95:01:EF:D8	2	TftpReqRcvd	0	13	6868	1736	513622	144655	19	0	0
00:90:83:32:9F:8C	2	Registered	0	34788	1244	34782	89916	2313518	86633	0	0
00:90:83:36:82:EE	2	Registered	0	8892	1692	8886	125038	687924	88701	0	0
00:90:83:36:82:F1	2	Registered	0	8892	1692	8886	125038	687924	89404	0	0

Parameter Descriptions

This table describes the parameters in the summary window.

Table 20-3 Cable Modem Statistics Summary Window Parameters

Parameter	Description
MAC Address	The MAC address of the cable modem you want to view.
Upstream Channel ID	The upstream channel of the interface.

Parameter	Description
Status Value	The initialization status of the specific cable modem.
CPEs	The number of customer premise equipment devices attached behind the specific cable modem.
Packets	The cumulative number of Packet Data packets received by the cable modem.
US Packets	The number of upstream channel Packet Data packets received by the cable modem.
DS Packets	The number of downstream channel Packet Data packets received by the cable modem.
US Bytes	The number of upstream channel bits received by the cable modem.
DS Bytes	The number of downstream channel bits received by the cable modem.
Non Errors	The number of codewords received without error from the cable modem.
Corrected Errors	The number of codewords received with correctable errors from the cable modem.
Uncorrectable Errors	The number of codewords received with uncorrectable errors from the cable modem.

Monitoring Cable Modem Services Information

The function of CMTS Cable Modems Services is to monitor the cable modem (CM) status and QoS Profile that have been assigned to DOCSIS 1.0 cable modems. These services are assigned when the cable modems are provisioned. *For more information about provisioning cable modems, refer to the FastFlow Broadband Provisioning Manager Guide, or the documentation for your external provisioning manager.*

Cable modems, within the CMTS Cable Modems Services window, are identified by their Service ID (SID). From this window, the MAC address and cable modem status information can be displayed for a specific SID. The cable modem QoS Profile information can also be displayed for a specific SID.

Before You Begin

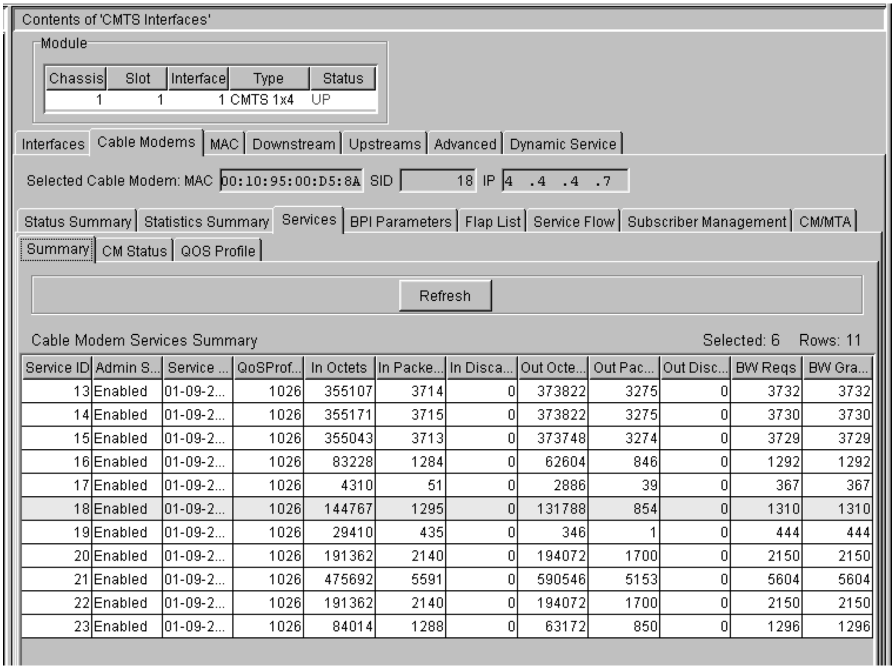
Before you monitor services, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **CMTS** > **Interfaces**.
2. Click **Cable Modems** tab.
3. Click **Services** tab.
4. Click **Summary** tab (Figure 20-5, "Cable Modem Services Summary Window").
5. Select the row that includes the SID that you wish to display.
6. Click **Refresh** to update the information.

NOTE: Within Services, you may view a list of the provisioned DOCSIS 1.0 and 1.1 cable modems. However, you may only monitor CM Status and QoS Profiles for DOCSIS 1.0 cable modems. To monitor services for DOCSIS 1.1 cable modems, refer to section "Monitoring Quality of Service" on page 587.

What You See

Figure 20-5 Cable Modem Services Summary Window



Contents of 'CMTS Interfaces'

Module

Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

Selected Cable Modem: MAC 00:10:95:00:D5:8A SID 18 IP 4 .4 .4 .7

Cable Modem Services Summary Selected: 6 Rows: 11

Service ID	Admin S...	Service ...	QoSProf...	In Octets	In Packe...	In Disca...	Out Octe...	Out Pac...	Out Disc...	BW Reqs	BW Gra...
13	Enabled	01-09-2...	1026	355107	3714	0	373822	3275	0	3732	3732
14	Enabled	01-09-2...	1026	355171	3715	0	373822	3275	0	3730	3730
15	Enabled	01-09-2...	1026	355043	3713	0	373748	3274	0	3729	3729
16	Enabled	01-09-2...	1026	83228	1284	0	62604	846	0	1292	1292
17	Enabled	01-09-2...	1026	4310	51	0	2886	39	0	367	367
18	Enabled	01-09-2...	1026	144767	1295	0	131788	854	0	1310	1310
19	Enabled	01-09-2...	1026	29410	435	0	346	1	0	444	444
20	Enabled	01-09-2...	1026	191362	2140	0	194072	1700	0	2150	2150
21	Enabled	01-09-2...	1026	475692	5591	0	590546	5153	0	5604	5604
22	Enabled	01-09-2...	1026	191362	2140	0	194072	1700	0	2150	2150
23	Enabled	01-09-2...	1026	84014	1288	0	63172	850	0	1296	1296

Parameter Descriptions

This table provides a description of the Services Summary Window

Table 20-4 Cable Modem Services Summary Window Parameters.

Parameter	Description
Service ID (SID)	SID assigned dynamically to the cable modem by the CMTS. A cable modem keeps the same SID assignment for as long as it continues to Range and is Registered with the CMTS. For example, if a cable modem is reset or goes through a power cycle, CMTS reassigns the next available SID number to the cable modem the next time it ranges and registers.
Service Create Time	Date and time at which the SID was assigned to the cable modem.
Admin Status	Status of the Service assigned to the cable modem.
QoS Profile	Name of the QoS Profile provisioned to this cable modem.

Parameter	Description
In Octets	Number of bytes received from this cable modem.
In Packets	Number of packets received from this cable modem.
In Discards	Aggregate number of discard packets received.
Out Octets	Number of bytes transmitted to this cable modem.
Out Packets	Number of packets transmitted to this cable modem.
Out Discards	Aggregate number of discard packets transmitted.
BW Reqs	Number of bandwidth requests received from this cable modem.
BW Grants	Number of bandwidth requests transmitted to this cable modem.

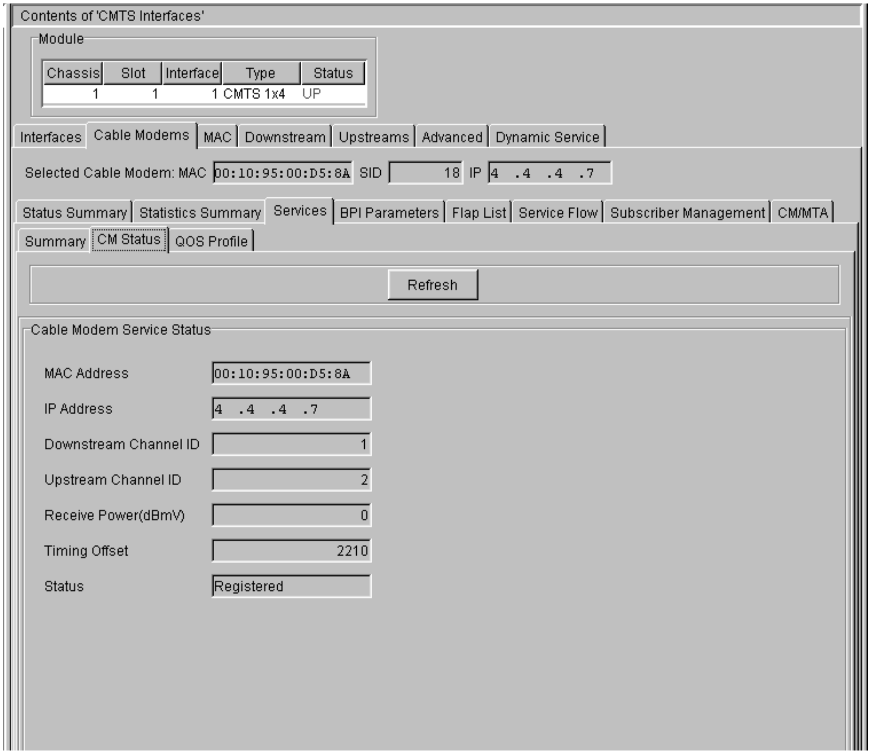
Viewing Cable Modem (CM) Status

To view CM status for a DOCSIS 1.0 cable modem, follow this procedure:

1. In the Cable Modems window, click the **Services** tab.
2. Select the row that includes the desired Service ID (Figure 20-5, "Cable Modem Services Summary Window").
3. Click the **CM Status** tab.
4. Click **Refresh** to update the information.

What You See

Figure 20-6 CM Status Window



Contents of 'CMTS Interfaces'

Module

Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

Selected Cable Modem: MAC 00:10:95:00:D5:8A SID 18 IP 4 .4 .4 .7

Cable Modem Service Status

MAC Address	00:10:95:00:D5:8A
IP Address	4 .4 .4 .7
Downstream Channel ID	1
Upstream Channel ID	2
Receive Power(dBmV)	0
Timing Offset	2210
Status	Registered

Parameter Descriptions

This table provides a description of the CM Status window.

Table 20-5 CM Status Window Parameters

Parameter	Description
MAC Address	RF MAC address of this cable modem
IP Address	IP address assigned to this cable modem by DHCP.
Downstream Channel ID	Cuda 12000 supports only one downstream channel. By default, Downstream Channel is set at 1.
Upstream Channel ID	Upstream channel assigned to the cable modem.

Parameter	Description
Receive Power (dBmV)	Receive power level from the CMTS for the upstream interface from the cable modem. By default, the Receive Power is set at 0, which is the optimal setting for the upstream power level. Acceptable values are -160 to 260 TenthdBmV. The Receive Power is dependent on the selected channel-width.
Timing Offset	Measure of the current round-trip time for this cable modem. Timing Offset is used for timing cable modem upstream transmissions to ensure synchronized arrivals at the CMTS. Units are in terms of (6.25 microseconds/64). A value of zero is returned if the time is unknown.
Status	Current cable modem connectivity state specified in the RF Interface Specification. Returned status information is the cable modem status as assumed by the CMTS. Following describes the status value events that are monitored:
InitRngRcvd	CMTS received an Initial Ranging Request message from the cable modem and the initial ranging process is not yet complete.
Ranging	Modem is in the process of ranging.
RangingComplete	CMTS sent a Range Response (success) message to the cable modem.
DhcpDiscRcvd	CMTS has received a DHCP Discover message from the cable modem.
DhcpReqRcvd	CMTS has received a DHCP Request from the cable modem.
TimeReqRcvd	CMTS has received a Time Request.
TftpReqRcvd	CMTS has received a TFTP Request from the cable modem.
Registered	Cable modem is registered, without Baseline Privacy.
RegNoNetAccess	Cable modem is registered, but Network Access is disabled.
RegBpiKek	Cable modem is registered, with Baseline Privacy enable. A Key Encryption Key has been assigned.
RegBpiTek	Cable modem is registered, with Baseline Privacy enable. A Traffic Encryption Key has been assigned.
RegFailBadMic	Modem registration failed, due to CMTS MIC comparison failure.
RegFailBadCos	Modem registration failed, due to class of service failure.

Parameter	Description
RegFailAuth	Modem registration failed, due to authorization failure.
RegKekReject	Cable modem is registered, with Baseline Privacy enabled. A Key Encryption Key has been rejected.
RegTekReject	Cable modem is registered, with Baseline Privacy enabled. A Traffic Encryption Key has been rejected.

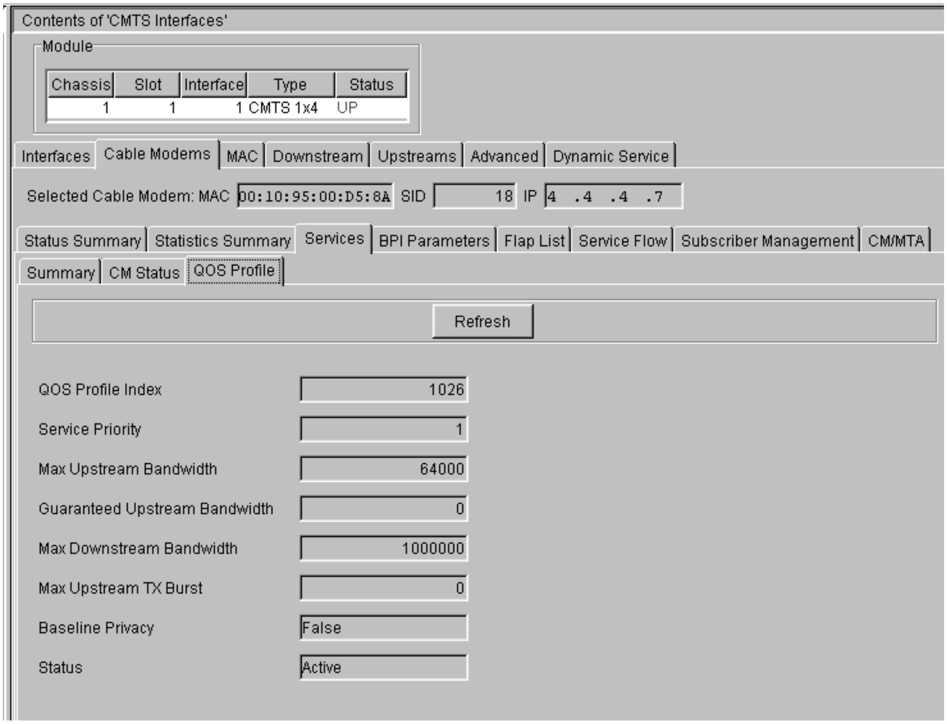
Viewing a QoS Profile

The QoS Profile window displays the QoS Profile, by Service ID, for the DOCSIS 1.0 cable modem that you selected from within the CM Status Summary display.

To view a QoS profile, follow this procedure:

1. In the Cable Modems window, click the **Services** tab.
2. Select the row that includes the Service ID for the DOCSIS 1.0 cable modem (Figure 20-5, “Cable Modem Services Summary Window”).
3. Click the **QoS Profile** tab.
4. Click **Refresh** to update the information.

Figure 20-7 QOS Profile Window



Contents of 'CMTS Interfaces'

Module

Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

Selected Cable Modem: MAC 00:10:95:00:D5:8A SID 18 IP 4 .4 .4 .7

QOS Profile Index	1026
Service Priority	1
Max Upstream Bandwidth	64000
Guaranteed Upstream Bandwidth	0
Max Downstream Bandwidth	1000000
Max Upstream TX Burst	0
Baseline Privacy	False
Status	Active

Parameter Descriptions

This table describes the parameters in the QoS Profile window:

Table 20-6 QoS Profile Window Parameters

Parameter	Description
QOS Profile Index	The index of the QOS profile used by this cable modem service.
Service Priority	Priority for this service, ranging from 0 to 7, where a priority of 0 is lowest priority. This is the Service Class ID that is provisioned in Provisioning\QoS Profiles.
Max Upstream Bandwidth	Maximum upstream bandwidth in bits per second.
Guaranteed Upstream Bandwidth	Guaranteed upstream bandwidth in bits per second.

Parameter	**Description**
Max Downstream Bandwidth	Maximum downstream bandwidth in bits per second.
Max Upstream Tx Burst	This is the maximum number of bytes allowed to this user. The valid range is 0 to 65535. A value of zero implies there is no limit.
Baseline Privacy	Indicates whether or not Baseline Privacy is enabled. A value of “False” indicates that Baseline Privacy is disabled for this cable modem; a value of “True” indicates that Baseline Privacy is enabled for this cable.
Status	Indicates whether the QoS Profile is currently in use. A value of “Active” indicates that the profile is in use; a value of “Inactive” indicates that the profile is not in use.

Managing BPI Parameters

The Baseline Privacy Interface (BPI) protocol provides cable modems with data privacy across the Hybrid Fiber-Coaxial (HFC) network by encrypting traffic between cable modems and the CMTS.

NOTE: *For a cable modem to use BPI, you must configure the Baseline Privacy settings in the modem configuration file. This file downloads during the transfer of operation parameters.You create configuration files within the cable modem provisioning process. Refer to the FastFlow Broadband Provisioning Manager CLI-based Administration Guide, or the guide of your external provisioning manager.*

BPI provides authorization parameters and Traffic Encryption Keys (TEKs) that secure traffic between cable modems and the CMTS.

During the CMTS registration process, the CMTS assigns one or more static Service Identifiers (SIDs) to the registering cable modem that matches the cable modems class-of-service provisioning. The first static SID that the CMTS assigns is the primary SID and serves as the cable modem’s primary Security Association Identifier (SAID).

After successfully completing authentication and authorization with the CMTS, the cable modem sends a request to the CMTS requesting TEKs to use with each of the SAIDs. The CMTS response contains the TEKs.

Monitoring BPI includes the following tasks:

- Viewing Privacy Authorizations
- Configuring Privacy Authorizations.
- Viewing an Authorization X.509 Certificate
- Viewing privacy keys.

Before You Begin

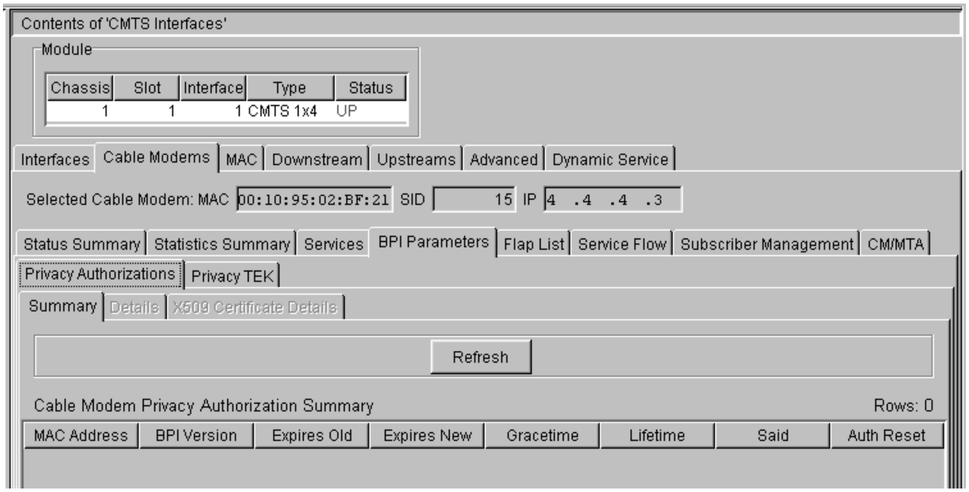
Before you begin to manage privacy authorizations and TEK, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **CMTS** > **Interfaces.**
2. Click the **Interfaces** tab. Select the interface that you want to view or configure.

3. Click the **Cable Modems** tab.
4. Click the **BPI Parameters** tab.

What You See

Figure 20-8 BPI Parameters Window



Contents of 'CMTS Interfaces'

Module

Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

Selected Cable Modem: MAC 00:10:95:02:BF:21 SID 15 IP 4 .4 .4 .3

Cable Modem Privacy Authorization Summary Rows: 0

MAC Address	BPI Version	Expires Old	Expires New	Gracetime	Lifetime	Said	Auth Reset

Viewing Privacy Authorizations

You can display lifetime in seconds for all new authorizations, as well as for existing authorizations for a specified interface or a specified cable modem.

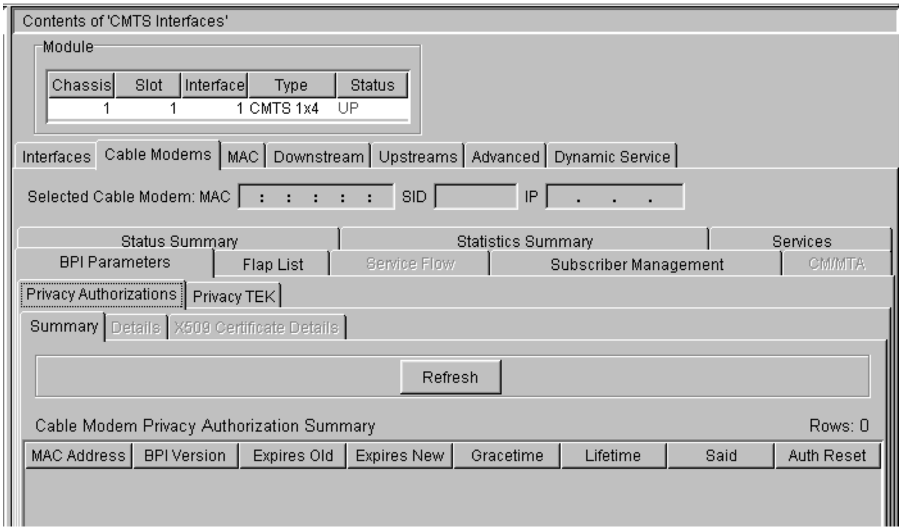
To view privacy authorizations, follow this procedure:

5. In the BPI Parameters window, click the **Privacy Authorizations** tab.
6. Click the **Summary** tab. The Summary window appears.
7. Click **Refresh** to update the information.

What You See

This figure shows an example of the Summary window

Figure 20-9 Privacy Authorizations Summary Window.



Contents of 'CMTS Interfaces'

Module

Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

Selected Cable Modem: MAC : : : : : SID IP . . .

Cable Modem Privacy Authorization Summary Rows: 0

MAC Address	BPI Version	Expires Old	Expires New	Gracetime	Lifetime	Said	Auth Reset

Parameter Descriptions

This table provides a description of the Summary window parameters.

Table 20-7 Privacy Authorizations Summary Window Parameters

Parameter	Description
MAC Address	Read only. Physical address of the cable modem to which the authorization association applies.
BPI Version	Read only. Version of Baseline Privacy that the cable modem is operating. The options are bpi or bpiplus.
Expires Old	Read only. Actual clock time when the immediate predecessor of the most recent authorization expires for this cable modem. If this cable modem does not have active authorization, the value is the expiration date and time of the last active authorization.
Expires New	Read only. Actual clock time when the most recent authorization for this cable modem expires. If this cable modem does not have an active authorization, the value is the expiration date and time of the last active authorization.
Gracetime	Read only. Grace time, in seconds, for the authorization key.
Lifetime	Read only. Lifetime, in seconds, the CMTS assigns to an authorization key for this cable modem.

Parameter	Description
Said	Read only. Indicates the Security Association Identifier (SAID)
Authorization Reset	Indicates when the cable modem resets. The options are:
NoResetRequested	Cable modem has not reset since the last CMTS reboot.
InvalidateAuth	CMTS invalidates the current cable modem authorization keys, but does not transmit an authorization message or invalidates unicast TEKs.
sendAuthInvalid	CMTS invalidates the current cable modem authorization key and transmits an invalid message to the cable modem. The CMTS does not invalidate the unicast TEKs.
InvaliddateTEKs	CMTS invalidates the current authorization key and transmits an authorization invalid message to the cable modem. The CMTS also invalidates all unicast TEKs associated with this cable modem authorization.

Configuring Privacy Authorizations

You can configure lifetime in seconds for all new authorizations, as well as for existing authorizations for a specified interface or a specified cable modem.

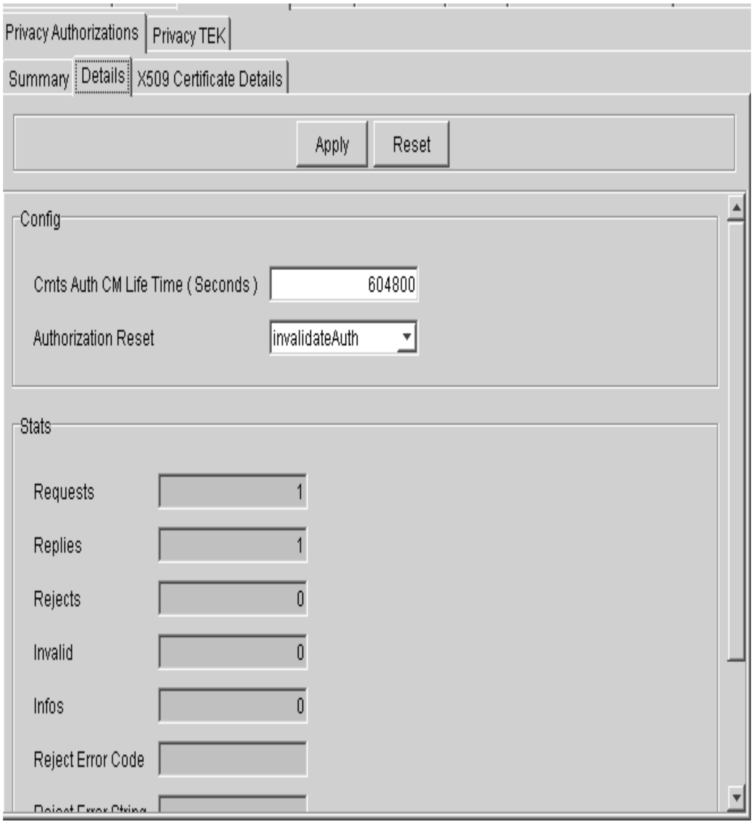
To configure privacy authorizations, follow this procedure.

1. In the BPI Parameters window, click the **Privacy Authorizations** tab.
2. Click the **Summary** tab. The Summary window appears.
3. Select the cable modem that you wish to configure.
4. Click the **Details** tab.
5. Enter values for the parameters. Refer to Table 20-8.
6. Click **Apply** to commit the information or click **Reset** to return to the default values.

What You See

This figure shows an example of the Details window.

Figure 20-10 Privacy Authorization Details Window



Cmts Auth CM Life Time (Seconds) 604800

Authorization Reset invalidateAuth

Requests 1

Replies 1

Rejects 0

Invalid 0

Infos 0

Reject Error Code

Reject Error String

Parameter Descriptions

This table provides a description of the Details window parameters.

Table 20-8 Privacy Authorizations Details Window Parameters

Parameter	Description
Cmts Auth CM Life Time (seconds)	Read only. Lifetime, in seconds, the CMTS assigns to an authorization key for this cable modem.
Authorization Reset	Indicates when the cable modem resets. The options are:
NoResetRequested	Cable modem has not reset since the last CMTS reboot.

Parameter	Description
InvalidateAuth	CMTS invalidates the current cable modem authorization keys, but does not transmit an authorization message or invalidates unicast TEKs.
sendAuthInvalid	CMTS invalidates the current cable modem authorization key and transmits an invalid message to the cable modem. The CMTS does not invalidate the unicast TEKs.
InvaliddateTEKs	CMTS invalidates the current authorization key and transmits an authorization invalid message to the cable modem. The CMTS also invalidates all unicast TEKs associated with this cable modem authorization.
Requests	Read only. Number of times the CMTS receives an authorization request message from this cable modem.
Replies	Read only. Number of times the CMTS transmits an authorization reply message to this cable modem.
Rejects	Read only. Number of times the CMTS transmits an authorization reject message to this cable modem.
Invalids	Read only. Number of times the CMTS transmits an authorization invalid message to this cable modem.
Infos	Read only. Number of times the CMTS receives an authorization information message from this cable modem.
Reject Err Code	Read only. Error code in the most recent authorization reject message that transmits to the cable modem.
None	No authorization message transmits to the cable modem.
Unknown	Last error code was zero.
UnauthorizedCM	Cable modem is not authorized.
UnauthorizedSAID	Cable modem does not have an authorized SAID.
PermanentAuth Failure	Error is of a permanent nature.
Time of Day Not Acquired	Cable modem does not have proper time of day parameter.
Reject Error String	Read only. Most recent authorization message that transmits to the cable modem. If the string is of zero length, no authorization reject messages transmit to the cable modem.

Parameter	Description
Invalid Error Code	Error code in the most recent authorization invalid message that transmits to the cable modem.
None	No authorization message transmits to the cable modem.
Unknown	Last error code was zero.
Unauthorizedcm	Cable modem does not have authorization.
Unsolicited	
InvalidKey Sequence	
KeyRequestAuth Failure	
Invalid Error String	Read only. Display string in the most recent authorization reject message that transmits to the cable modem. If the string is of zero length, no authorization reject message transmits to the cable modem.

Viewing an Authorization X.509 Certificate

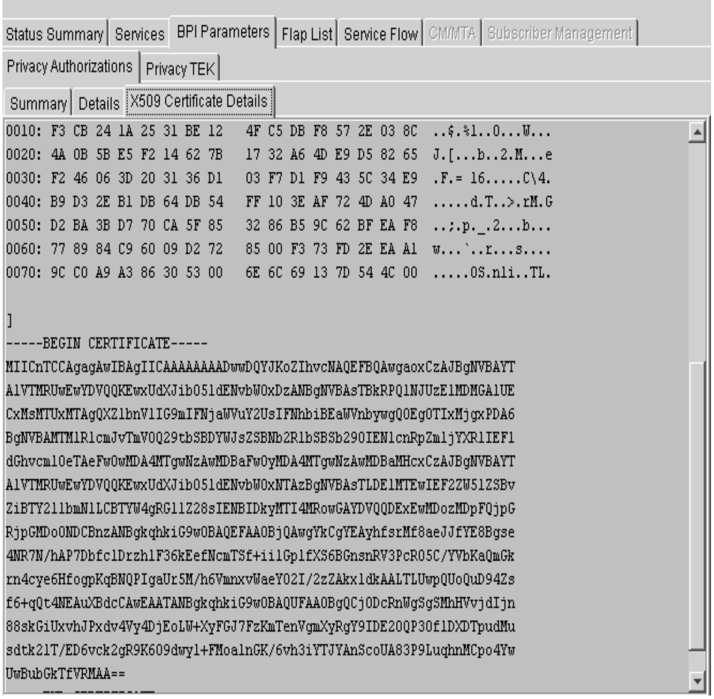
BPI uses the X.509 digital certificates to authenticate key exchanges between the cable modem and CMTS. To view the X.509 certificate details, follow this procedure:

1. In the BPI Parameters window, click the **Privacy Authorizations** window.
2. Click the **Summary** tab. The Summary window appears.
3. Select the modem that you wish to view.
4. Click the **X509 Certificate Details** tab. The certificate information appears.

What You See

This figure shows an example of the X509 Certificate Details window.

Figure 20-11 Privacy Authorizations X509 Certificate Details



```
0010: F3 CB 24 1A 25 31 BE 12   4F C5 DB F8 57 2E 03 8C  ..$.%1..O...W...
0020: 4A 0B 5B E5 F2 14 62 7B   17 32 A6 4D E9 D5 82 65  J.[...b..2.M...e
0030: F2 46 06 3D 20 31 36 D1   03 F7 D1 F9 43 5C 34 E9  .F.= 16.....C\4.
0040: B9 D3 2E B1 DB 64 DB 54   FF 10 3E AF 72 4D A0 47  .....d.T..>.rM.G
0050: D2 BA 3B D7 70 CA 5F 85   32 86 B5 9C 62 BF EA F8  ..;.p._.2...b...
0060: 77 89 84 C9 60 09 D2 72   85 00 F3 73 FD 2E EA A1  w...`..r...s....
0070: 9C C0 A9 A3 86 30 53 00   6E 6C 69 13 7D 54 4C 00  .....0S.nli..TL.


]
-----BEGIN CERTIFICATE-----
```

```
MIICnTCCAgagAwIBAgIICAAAAAAAADwwDQYJKoZIhvcNAQEFBQAwgaoxCzAJBgNVBAYT
AlVTMRUwEwYDVQQKEwxUdXJib05ldENvbW0xDzANBgNVBAsTBkRPQ1NJUzE1MDMGA1UE
CxMsMTUxMTAgQXZlbnVlIG9mIFNjaWVuY2UsIFNhbiBEaWVnbywgQ0EgOTIxMjgxPDA6
BgNVBAMTMlRlcmJvTmV0Q29tbSBDYWJsZSBNb2RlbSBSb290IENlcnRpZmljYXRlIEF1
dGhvcml0eTAeFw0wMDA4MTgwNzAwMDBaFw0yMDA4MTgwNzAwMDBaMHcxCzAJBgNVBAYT
AlVTMRUwEwYDVQQKEwxUdXJib05ldENvbW0xNTAzBgNVBAsTLDE1MTEwIEF2ZW51ZSBv
ZiBTY2llbmNlLCBTYW4gRGllZ28sIENBIDkyMTI4MRowGAYDVQQDExEwMDozMDpFQjpG
RjpGMDo0NDCBnzANBgkqhkiG9w0BAQEFAA0BjQAwgYkCgYEAyhfsrMf8aeJJfYE8Bgse
4NR7N/hAP7DbfclDrzhlF36kEefNcmTSf+iilGplfXS6BGnsnRV3PcR05C/YVbKaQmGk
rn4cye6HfogpKqBNQPIgaUr5M/h6VmnxvWaeYO2I/2zZAkxldkAALTLUwpQUoQuD94Zs
f6+qQt4NEAuXBdcCAwEAATANBgkqhkiG9w0BAQUFAA0BgQCj0DcRnWgSgSMhHVvjdIjn
88skGiUxvhJPxdv4Vy4DjEoLW+XyFGJ7FzKmTenVgmXyRgY9IDE20QP30flDXDTpudMu
sdtk2lT/ED6vck2gR9K609dwyl+FMoalnGK/6vh3iYTJYAnScoUA83P9LuqhnMCpo4Yw
UwBubGkTfVRMAA==
```

Viewing Privacy TEK

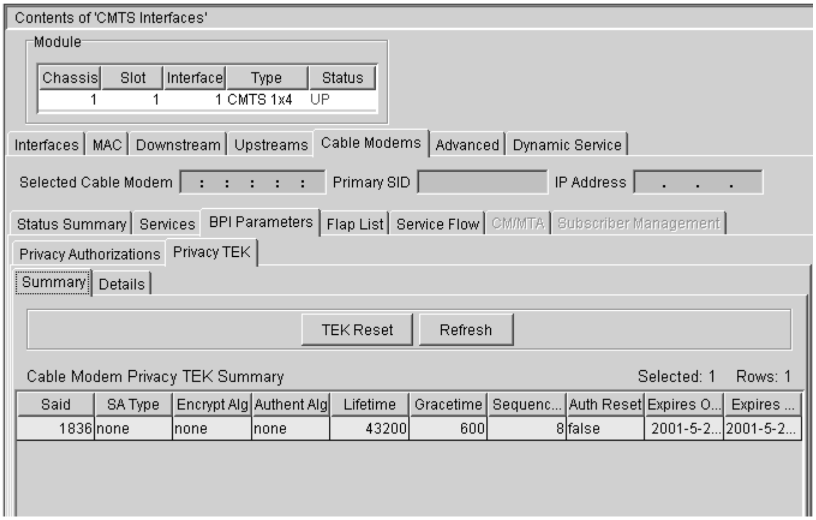
For cable modems configured on a particular CMTS interface, you can view the Traffic Encryption Key (TEK) parameters.

To view summary information for privacy TEKs, follow this procedure:

1. In the BPI Parameters window, click the **Privacy TEKs** tab. The Privacy TEKs window appears.
2. Click the **Summary** tab. The Summary window appears.
3. Click **Refresh** to update the information.

What You See

Figure 20-12 Summary window.



Contents of 'CMTS Interfaces'

Module

Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

Selected Cable Modem : : : : : Primary SID IP Address . . .

Cable Modem Privacy TEK Summary Selected: 1 Rows: 1

Said	SA Type	Encrypt Alg	Authent Alg	Lifetime	Gracetime	Sequenc...	Auth Reset	Expires O...	Expires ...
1836	none	none	none	43200	600	8	false	2001-5-2...	2001-5-2...

Parameter Descriptions

This table provides a description of the Summary window.

Table 20-9 .Privacy TEK Summary Window Parameters

Parameter	Description
SAID	Value is the DOCSIS Security Association Identifier (SAID)
SA Type	Type of security association. The options are:

Parameter	Description
None	No security.
Primary	
Static	
Dynamic	
Encrypt Alg	Read only. Type of Data encryption algorithm. The options are:
None	No algorithm in use.
Des56CbCMode	Indicates a 56-bit Data Encryption Standard (DES) using Cypher Block Chaining (CBC) mode.
Des40CbcMode	Indicates a 40-bit DES using CBC mode.
Auth Alog	Read only. Type of Data authentication algorithm.
Lifetime	Lifetime, in seconds, the CMTS assigns to keys for this TEK association. The range is 1 to 604800.
Gracetime	Grace time, in seconds, for the TEK.
Sequence Num	Most recent TEK key sequence number for this SAID.
Auth Reset	Indicates the status of the TEK.
True	CMTS invalidates the current active TEK and generates a new TEK for the associated SAID. The CMTS may also generate an unsolicited TEK invalid message.
False	CMTS does not invalidate the current TEK.
Expires Old	Actual clock time when the most recent authorization expires. If this cable modem does not have active authorization, the value is the expiration date and time of the last active authorization.
Expires New	Actual clock time the most recent authorization for this cable modem expires. If this cable modem does not have an active authorization, the value is the expiration date and time of the last active authorization.

Configuring Privacy TEK

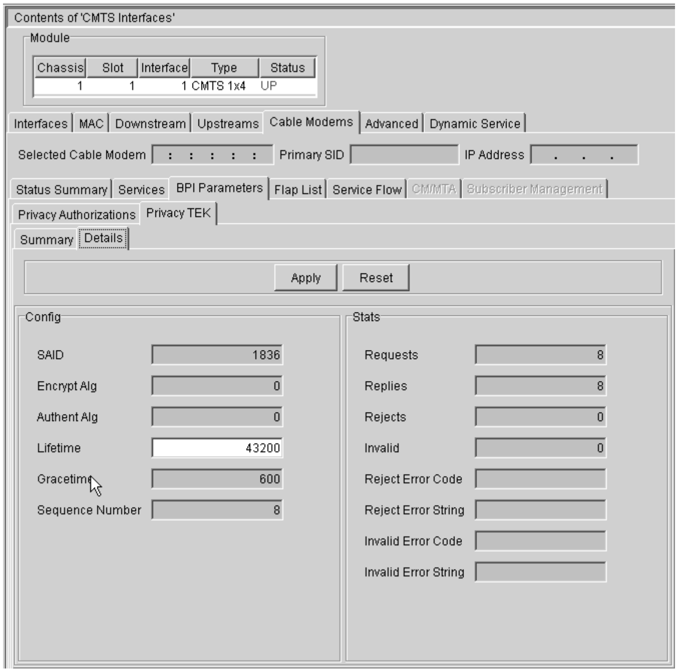
To configure privacy TEKs for cable modems, follow this procedure:

1. In the BPI Parameters window, click the **Privacy TEK** tab. The **Privacy TEK** window appear.s
2. Click the **Summary** tab. The Summary window appears.
3. Select the modem that you wish to configure.
4. Click the **Details** tab. The Details window appears. Refer toTable 20-10.
5. Enter values for the parameters.
6. Click **Apply** to commit the information or click **Reset** to return to the default values.

What You See

This figure shows an example of the Details window.

Figure 20-13 Privacy TEK Details Window



Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

Selected Cable Modem : : : : :   Primary SID   IP Address . . .

SAID	1836
Encrypt Alg	0
Authent Alg	0
Lifetime	43200
Gracetime	600
Sequence Number	8

Requests	8
Replies	8
Rejects	0
Invalid	0
Reject Error Code	
Reject Error String	
Invalid Error Code	
Invalid Error String	

Parameter Descriptions

This table provides a description of the Details window parameters.

Table 20-10 Privacy TEK Details Window Parameters

Parameter	Description
SAID	Value is the DOCSIS Security Association Identifier (SAID)
Encrypt Alg	Read only. Type of Data encryption algorithm. The options are:
None	No algorithm in use.
Des56CbCMode	Indicates a 56-bit Data Encryption Standard (DES) using Cypher Block Chaining (CBC) mode.
Des40CbcMode	Indicates a 40-bit DES using CBC mode.
Auth Alog	Read only. Type of Data authentication algorithm. The options are:
Lifetime	Lifetime, in seconds, the CMTS assigns to keys for this TEK association. The range is 1 to 604800.
Gracetime	Grace time, in seconds, for the TEK.
Sequence Num	Most recent TEK key sequence number for this SAID.
Requests	Read only. Number of times the CMTS receives an authorization request message from this cable modem.
Replies	Read only. Number of times the CMTS transmits an authorization reply message to this cable modem.
Rejects	Read only. Number of times the CMTS transmits an authorization reject message to this cable modem.
Invalids	Read only. Number of times the CMTS transmits an authorization invalid message to this cable modem.
Reject Err Code	Read only. Error code in the most recent authorization reject message that transmits to the cable modem.
None	No authorization message transmits to the cable modem.
Unknown	Last error code was zero.
UnauthorizedCM	Cable modem is not authorized.
UnauthorizedSAID	Cable modem does not have an authorized SAID.

Parameter	Description
PermanentAuth Failure	Error is of a permanent nature.
Time of Day Not Acquired	Cable modem does not have proper time of day parameter.
Reject Error String	Read only. Most recent authorization message that transmits to the cable modem. If the string is of zero length, no authorization reject messages transmits to the cable modem.
Invalid Error Code	Error code in the most recent authorization invalid message that transmits to the cable modem.
None	No authorization message transmits to the cable modem.
Unknown	Last error code was zero.
Unauthorizedcm	Cable modem does not have authorization.
Unsolicited	
InvalidKey Sequence	
KeyRequestAuth Failure	
Invalid Error String	Read only. Display string in the most recent authorization reject message that transmits to the cable modem. If the string is of zero length, no authorization reject message transmits to the cable modem.

Monitoring the Flap List

The flap list monitors the cable modems that have connectivity problems. Flapping refers to the rapid disconnecting and reconnecting of a cable modem that has problems holding a connection.

The function of the flap list includes:

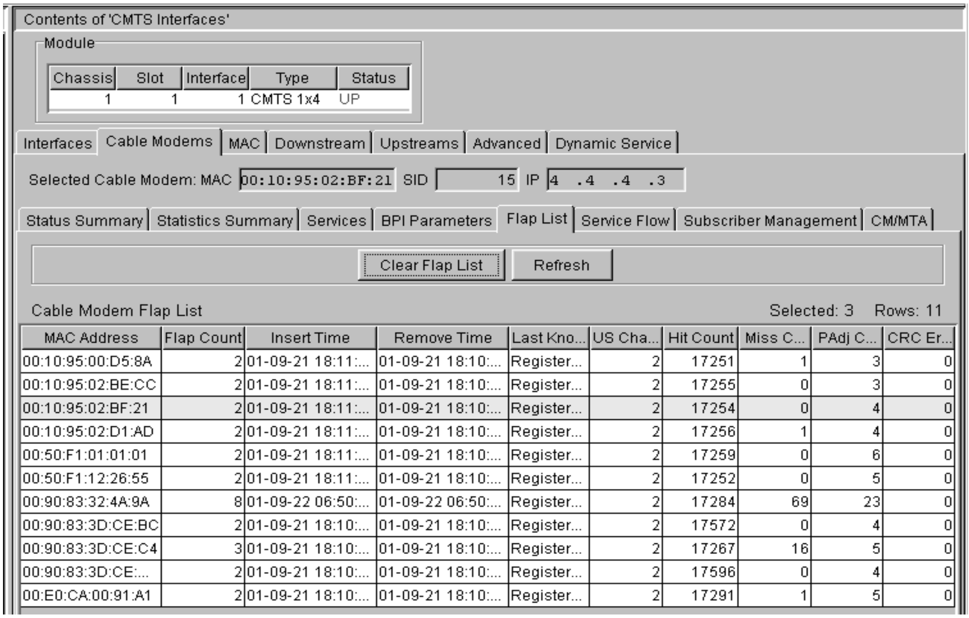
- Maintaining entries for cable modems that completed registration and subsequently reset.
- By MAC Address, logging the time of the most recent activity of the cable modem.

To monitor the flap list, follow this procedure:

1. In the Cable Modems window, click the **Flap List** tab.
2. Click **Refresh** to update the information.

What You See

Figure 20-14 Flap List Window



Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

Selected Cable Modem: MAC 00:10:95:02:BF:21 SID 15 IP 4 .4 .4 .3

Cable Modem Flap List

Selected: 3 Rows: 11

MAC Address	Flap Count	Insert Time	Remove Time	Last Kno...	US Cha...	Hit Count	Miss C...	PAdj C...	CRC Er...
00:10:95:00:D5:8A	2	01-09-21 18:11:...	01-09-21 18:10:...	Register...	2	17251	1	3	0
00:10:95:02:BE:CC	2	01-09-21 18:11:...	01-09-21 18:10:...	Register...	2	17255	0	3	0
00:10:95:02:BF:21	2	01-09-21 18:11:...	01-09-21 18:10:...	Register...	2	17254	0	4	0
00:10:95:02:D1:AD	2	01-09-21 18:11:...	01-09-21 18:10:...	Register...	2	17256	1	4	0
00:50:F1:01:01:01	2	01-09-21 18:11:...	01-09-21 18:10:...	Register...	2	17259	0	6	0
00:50:F1:12:26:55	2	01-09-21 18:11:...	01-09-21 18:10:...	Register...	2	17252	0	5	0
00:90:83:32:4A:9A	8	01-09-22 06:50:...	01-09-22 06:50:...	Register...	2	17284	69	23	0
00:90:83:3D:CE:BC	2	01-09-21 18:10:...	01-09-21 18:10:...	Register...	2	17572	0	4	0
00:90:83:3D:CE:C4	3	01-09-21 18:10:...	01-09-21 18:10:...	Register...	2	17267	16	5	0
00:90:83:3D:CE:...	2	01-09-21 18:10:...	01-09-21 18:10:...	Register...	2	17596	0	4	0
00:E0:CA:00:91:A1	2	01-09-21 18:10:...	01-09-21 18:10:...	Register...	2	17291	1	5	0

Parameter Descriptions

This table describes the parameters in the Flap List window:

Table 20-11 Flap List window parameters:.

Parameter	Description
MAC Address	RF MAC address of the cable modem.
Flap Count	Number of times that this cable modem reset from either the ranging complete or registration complete states.
Insert Time	Date and time that this cable modem was added to the flap list.
Remove Time	Last date and time that this cable modem reset.
Last Known State	Last state of the modem.
Hit Count	Number of times the modem responds to MAC layer keep alive messages. It can indicate intermittent upstream, laser clipping, or common-path distortion.
Miss Count	Specifies the number of times the cable modem misses the MAC layer keep alive messages. It can indicate intermittent upstream, laser clipping, or common-path distortion.
PAdj Count	Number of times the headend instructed the modem to adjust transmit power more than the threshold-specified number of dB. It can indicate amplifier degradation, poor connections, or thermal sensitivity.
CRC Errors Count	Number of Cyclic Redundancy Check errors from this cable modem. It can indicate intermittent upstream, laser clipping, or common-path distortion.

Monitoring Quality of Service

The Quality of Service (QoS) feature defines the transmission ordering and scheduling on the Radio Frequency Interface. It provides for both upstream and downstream traffic through the cable modem and CMTS. QoS classifies packets traversing the RF MAC interface into a Service Flow. The Cuda 12000 and cable modems provide this QoS by shaping, policing, and prioritizing traffic according to a parameter set defined for the Service Flow.

Service Flows

A Service Flow is unidirectional flow of packets transmitted either upstream by the cable modem or downstream by the CMTS. There are three types of services flows:

- Provisioned Service Flows
- Admitted Service Flows
- Active Service Flows

A Service Flow is characterized by the Service Flow ID, the service ID, the provisioned QoS parameter set, the admitted QoS parameter set, and the active QoS parameter set. It serves as the principal identifier in the cable modem and CMTS for the Service Flow.

Every Service Flow has a Service Flow Identifier (SFID) that the CMTS assigns. Active and admitted upstream Service Flows also have a service identifier (SID).

Classifiers

A classifier is a set of matching criteria that applies to each packet entering the cable network. It consists of some packet matching criteria, such as the destination IP address, a priority, and a reference to a Service Flow. Also, several classifiers may refer to the same Service Flow.

Incoming packets attempt to match to a classifier. If the packet matches one of the classifiers, it is forwarded to the Service Flow indicated by the SFID parameter in the classifier. If the packet does not match any of the classifiers, it is forwarded to the primary Service Flow.

Downstream classifiers apply to packets that the CMTS is transmitting and upstream classifiers apply to packets that the cable modem is transmitting.

Viewing Service Flows

At least two Service Flows per DOCSIS 1.1 cable modem configuration files must be defined, one for the upstream and one for the downstream. The first upstream Service Flow describes the primary upstream Service Flow and is the default Service Flow used for unclassified traffic. The first downstream Service Flow describes service to the primary downstream Service Flow.

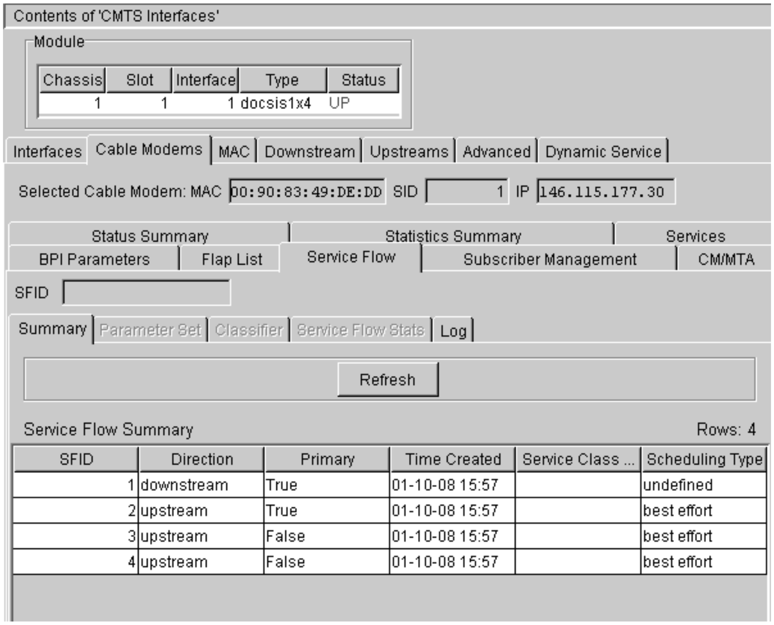
Before You Begin

To view defined Service Flows, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **CMTS** > **Interfaces.**
2. In the **Interfaces** window, select the interface that you want to view.
3. Click the **Cable Modems** tab.
4. Click the **Status Summary** tab. The **Status Summary** window appears.
5. Select the DOCSIS 1.1 cable modem for which you want to view.
6. Click the **Service Flow** tab. T
7. Click the **Summary** tab. All defined Service Flows for provisioned DOCSIS 1.1 cable modems are displayed.
8. Click **Refresh** to update the information.

What You See

Figure 5-1 Service Flow Summary Window



Contents of 'CMTS Interfaces'

Module

Chassis	Slot	Interface	Type	Status
1	1	1	docsis1x4	UP

Selected Cable Modem: MAC 00:90:83:49:DE:DD SID 1 IP 146.115.177.30

Service Flow Summary Rows: 4

SFID	Direction	Primary	Time Created	Service Class ...	Scheduling Type
1	downstream	True	01-10-08 15:57		undefined
2	upstream	True	01-10-08 15:57		best effort
3	upstream	False	01-10-08 15:57		best effort
4	upstream	False	01-10-08 15:57		best effort

Parameter Descriptions

This table provides a description of the Service Flow Summary window.

Table 20-12 Summary Window Parameters

Parameter	Description
SFID	A 32-bit identifier that the CMTS assigns to an admitted or active Service Flow. All Service Flows have a SFID. A value of zero indicates a SID does not associate with the Service Flow. Only active or admitted upstream Service Flows have a SID.
Direction	Direction of the Service Flow.
Primary	Indicates whether the Service Flow is the primary or secondary Service Flow.
Time Created	Creation time for the Service Flow.
Service Class Name	Name of the service class.

Table 20-12 Summary Window Parameters (continued)

Parameter	**Description**
Scheduling Type	Scheduling service the CMTS provides for an upstream Service Flow. The options are: undefined, best effort, non real time polling service, real time polling service, unsolicited grant service with AD, and unsolicited grant service.

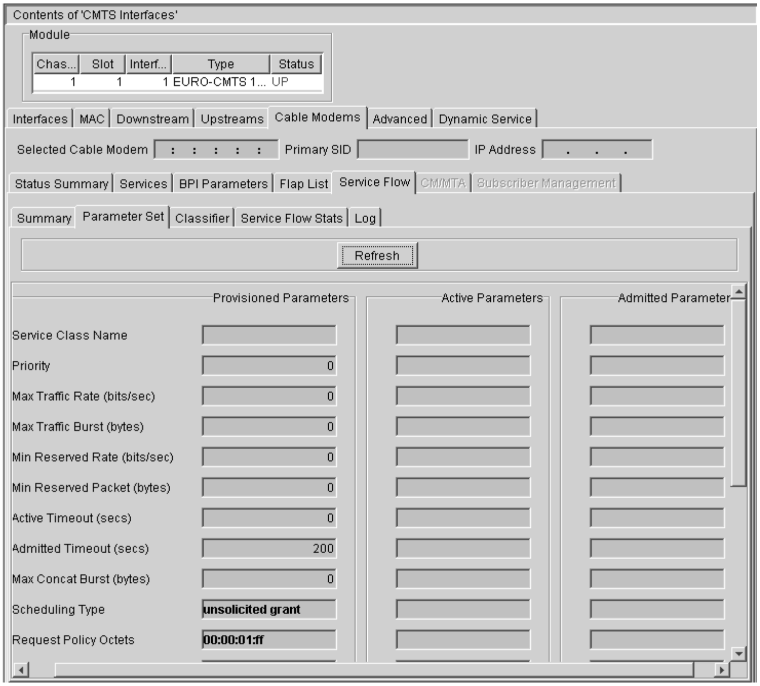
Viewing the Parameter Set

The parameter set describes the QoS attributes of a Service Flow or Service Class. It characterizes a Service Flow by providing the provisioned QoS parameter set, the admitted QoS parameter set, and the active QoS parameter set. To view the parameter set, follow this procedure:

1. In the **Summary** window, select the flow that you wish to view.
2. Click the **Parameter Set** tab. The **Parameter Set** window appears. The window displays the values for the provisioned, active, and admitted Service Flow:
   - **Provisioned Parameters** — QoS parameters that appear in the configuration file and are used for registration.
   - **Active Parameters** — QoS parameters that the service flow is providing to define the service.
   - **Admitted Parameters** — QoS parameters that the CMTS is reserving for future resources.
3. Click **Refresh** to update the information.

What You See

Parameter Set Window .



Contents of 'CMTS Interfaces'

Module

Chas...	Slot	Interf...	Type	Status
1	1	1	EURO-CMTS 1...	UP

Selected Cable Modem : : : : : Primary SID IP Address . . .

	Provisioned Parameters	Active Parameters	Admitted Parameter
Service Class Name			
Priority	0		
Max Traffic Rate (bits/sec)	0		
Max Traffic Burst (bytes)	0		
Min Reserved Rate (bits/sec)	0		
Min Reserved Packet (bytes)	0		
Active Timeout (secs)	0		
Admitted Timeout (secs)	200		
Max Concat Burst (bytes)	0		
Scheduling Type	unsolicited grant		
Request Policy Octets	00:00:01:ff		

Parameter Descriptions

This table provides a description of the **Parameter Set** window.

Table 20-13 Parameter Set Window Parameters

Parameter	Description
Service Class Name	Name that identifies the service class.
Priority	Relative priority of the Service Flow. Higher value indicates a higher priority.
Max Traffic Rate (bits/sec)	Maximum sustained traffic rate, in bits/sec, for this Service Flow. A value of zero indicates no maximum traffic rate is being enforced. This parameter applies to both upstream and downstream Service Flows.
Max Traffic burst (bytes)	Token bucket size, in bytes, for this parameter set. The max traffic burst size and the maximum traffic rate determine the maximum sustained traffic rate.

Table 20-13 Parameter Set Window Parameters (continued)

Parameter	Description
Min Reserved Rate (bits/sec)	Guaranteed minimum rate, in bits/sec, for this parameter set.
	The default is zero indicates no reserved bandwidth.
Min Reserved Packet (bytes)	Assumed minimum packet size, in bytes, for the minimum reserved rate.
Active Timeout (secs)	Maximum duration, in seconds, that resources remain unused on an active Service Flow before the CMTS signals that both active and admitted parameters are set to null.
	The default is zero to indicate an infinite amount of time.
Admitted Timeout	Maximum duration, in seconds, that resources remain in admitted state before being released. A value of zero indicates an infinite amount of time.
Max Concat Burst (bytes)	Maximum concatenated burst, in bytes, for an upstream Service Flow. A value of zero indicates no maximum burst.
Scheduling Type	Upstream scheduling service for an upstream Service Flow.
Request Policy Octets	Indicates the transmit interval opportunity the cable modem omits for upstream transmission request and packet transmissions.
	A value of one indicates the cable modem must not use an opportunity for transmission.
Nominal Polling Interval (usecs)	Nominal interval, in microseconds, between successive unicast request opportunities on an upstream Service Flow. This value is zero if this parameter does not apply to the scheduling type of the QoS parameter set or if the value is unknown.
Tolerable Poll Jitter (usecs)	Maximum amount of time, in microseconds, that the unicast request interval delays from the nominal periodic schedule on an upstream Service Flow.
Unsolicited Grant Size (bytes)	Unsolicited grant size, in bytes. It includes the entire MAC frame data PDU from the Frame Control byte to end of the MAC frame.
Nominal Grant Interval (usecs)	Nominal interval, in microseconds, between successive data grant opportunities on an upstream service flow.

Table 20-13 Parameter Set Window Parameters (continued)

Parameter	Description
Tolerable Grant Jitter (usecs)	Maximum amount of time, in microseconds, that the transmission opportunities delay from the nominal periodic schedule.
Grants Per Interval	Number of data grants per nominal grant interval.
TOS AND Mask	Specifies the AND mask for IP TOS byte for IP packets TOS value.
TOS OR Mask	Specifies the OR mask for IP TOS byte.
Max Latency (usecs)	Maximum latency between the reception of a packet by the CMTS on its network side interface (NSI) and the forwarding of the packet to the RF interface. A value of zero indicates no maximum latency. This parameter only applies to downstream Service Flows.
Bit Map	Indicates the set of QoS parameter set parameters actually signaled in the DOCSIS registration or dynamic service request message that creates the QoS parameter set.

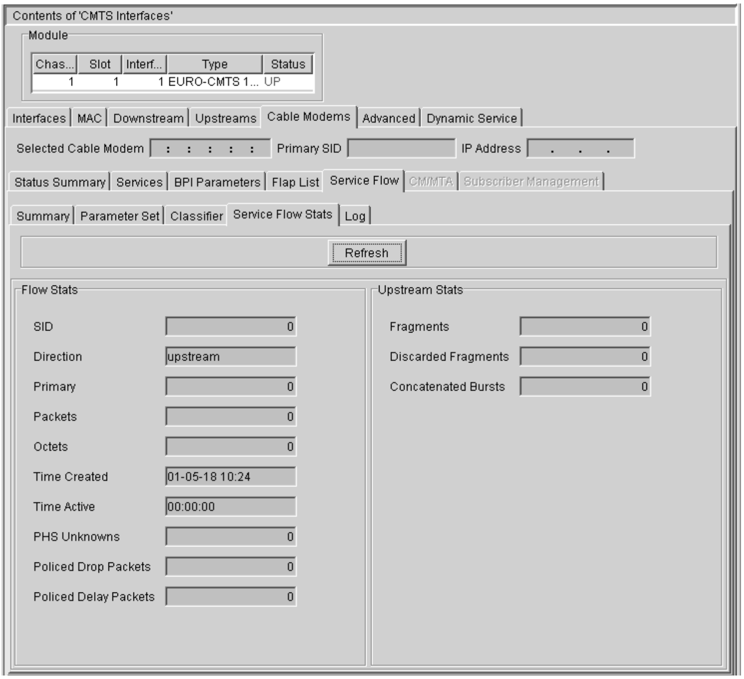
Viewing Service Flow Statistics

To view Service Flow statistics, follow this procedure:

1. In the **Summary** window, select the flow that you wish to view. Refer to Table 20-12.
2. Click the **Service Flow Stats** tab. The **Service Flow Stats** window appears. Refer to Table 20-14.
3. Click **Refresh** to update the window.

What You See

Figure 20-2 Service Flow Stats Window



Chas...	Slot	Interf...	Type	Status
1	1	1	EURO-CMTS 1...	UP

Selected Cable Modem : : : : :
Primary SID
IP Address . . .

Flow Stats

SID	0
Direction	upstream
Primary	0
Packets	0
Octets	0
Time Created	01-05-18 10:24
Time Active	00:00:00
PHS Unknowns	0
Policed Drop Packets	0
Policed Delay Packets	0

Upstream Stats

Fragments	0
Discarded Fragments	0
Concatenated Bursts	0

Parameter Descriptions

This table provides a description of the **Service Flow Stats** window.

Table 20-14 Service Flow Stats Window Parameters

Parameter	Description
Flow Stats	Provides statistics for Service Flows in a managed device.
SID	Identifier for a specific flow and indicates the direction of the packet: upstream or downstream.
Direction	Direction of the flow.
Primary	Indicates whether the Service Flow is the primary or secondary Service Flow.
Packets	Number of packets counted on this Service Flow.
Octets	Number of octets counted on this Service Flow after Payload Header Suppression (PHS).

Table 20-14 Service Flow Stats Window Parameters (continued)

Parameter	Description
Time Created	Creation time of the flow.
Time Active	Total time the Service Flow is active.
PHS Unknowns	Number of packets with an unknown payload header suppression index.
Policed Drop Packets	Number of packets the flow drops because of policing of the Service Flow, especially to limit the maximum rate of the flow.
Policed Delay Packets	Number of packets the flow delays because of policing of the Service Flow, especially to limit the maximum rate of the flow.
Upstream Stats	Provides statistics for the upstream Service Flows.
Fragments	Number of fragmentation headers the upstream Service Flow receives, regardless of whether the fragment was correctly re-assembled into a valid packet.
Discarded Fragments	Number of upstream fragments the flow discards and does bit assemble into a valid upstream packet.
Concatenated Bursts	Number of concatenation headers the upstream Service Flow receives.

Viewing Classifiers

You can configure the packet classification on a cable modem or CMTS. An incoming or outgoing packet attempts to match against the list of rules pertaining to the packet contents. A matching rule provides a SID to which the packet is classified. You can associate a Service Flow to 0 to 65535 classifiers, but you can only associate a classifier with one Service Flow.

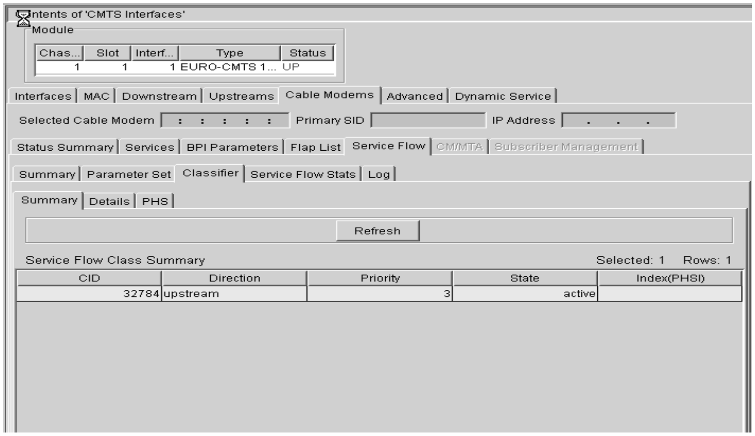
Viewing Classifier Summary

To view the classifier summary, follow this procedure:

1. In the **Summary** window, select the flow that you wish to configure.
2. Click the **Classifier** tab. The **Classifier** window appears.
3. Click the **Summary** tab. The **Summary** window appears.
4. Click **Refresh** to update the window.

What You See

Figure 20-3 Classifier Summary window



Module

Chas...	Slot	Interf...	Type	Status
1	1	1	EURO-CMTS 1...	UP

Selected Cable Modem : : : : : Primary SID IP Address . . .

Service Flow Class Summary Selected: 1 Rows: 1

CID	Direction	Priority	State	Index(PHSI)
32784	upstream	3	active	

Parameter Descriptions

This table provides a description of the Classifier Summary window.

Table 20-15 Summary Window Parameters

Parameter	Description
CID	Index for the packet classifier that the CMTS assigns.
Direction	Direction that the classifier applies.
Priority	Specifies the order of evaluation of the classifiers.
State	Indicates whether or not the classifier is currently classifying packets to a Service Flow.
Index (PHSI)	Unique index to identify references to the PHS rule for a given Service Flow.

Viewing Classifier Details

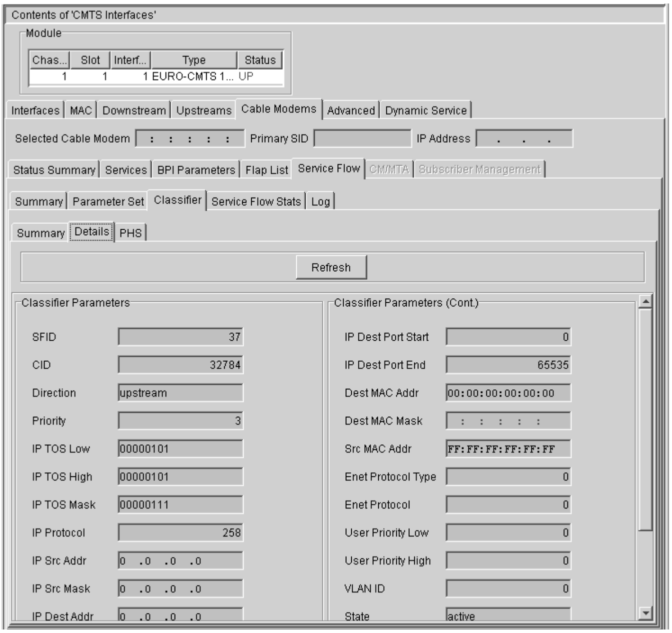
To view classifier details, follow this procedure:

1. In the **Summary** window, select the flow that you wish to view.
2. Click the **Classifier** tab. The **Classifier** window appears.
3. Click the **Details** tab. The **Details** window appears.

4. Click **Refresh** to update the information.

What You See

Figure 20-4 Classifier Details window



Chas...	Slot	Interf...	Type	Status
1	1	1	EURO-CMTS 1...	UP

Selected Cable Modem : : : : :   Primary SID   IP Address . . .

Classifier Parameters

SFID	37
CID	32784
Direction	upstream
Priority	3
IP TOS Low	00000101
IP TOS High	00000101
IP TOS Mask	00000111
IP Protocol	258
IP Src Addr	0 .0 .0 .0
IP Src Mask	0 .0 .0 .0
IP Dest Addr	0 .0 .0 .0

Classifier Parameters (Cont.)

IP Dest Port Start	0
IP Dest Port End	65535
Dest MAC Addr	00:00:00:00:00:00
Dest MAC Mask	: : : : :
Src MAC Addr	FF:FF:FF:FF:FF:FF
Enet Protocol Type	0
Enet Protocol	0
User Priority Low	0
User Priority High	0
VLAN ID	0
State	active

Parameter Descriptions

This table provides a description of the **Details** window.

Table 20-16 Details Window Parameters

Parameter	Description
SFID	Read only. The Service Flow Identifier.
CID	Read only. Unique identifier for the packet classifier that the CMTS assigns.
Direction	Read only. Indicates the direction for the classifier.

Table 20-16 Details Window Parameters (continued)

Parameter	Description
Priority	Indicates the order of evaluation for the classifiers. The higher the value, the higher the priority. A default value of zero is for provisioned Service Flow classifiers. A default value of 64 is for dynamic Service Flow classifiers.
IP TOS Low	Low value of a range of TOS byte values. If the referenced parameter is not present in the classifier, the value is zero.
IP TOS High	High value of a range of TOS byte values. If the referenced parameter is not present in the classifier, the value is zero.
IP TOS Mask	Mask value that ensures range checking of the TOS Low and TOS High values.
IP Protocol	Indicates the value of the IP protocol field necessary for IP packets to match this rule. A value of 256 matches traffic with any IP protocol value. A value of 257 matches both TCP and UDP. If the referenced parameter is not present in the classifier, the value is 258.
IP Src Addr	Indicates the value of the IP source address necessary for packets to match this rule.
IP Src Mask	Specifies the bits of a packet's IP source address to compare when matching this rule.
IP Dest Addr	Specifies the low end inclusive range of TCP/UDP source port numbers to which the packet compares. This parameter is ignored for non-TCP/UDP IP packets. If the referenced parameter is not present in the classifier, the value is zero.
IP Dest Mask	Specifies the bits of a packet's IP destination address to compare when matching this rule.
IP Src Port Start	Specifies the low and inclusive range of TCP/UDP source port numbers to which a packet compares.
IP Src Port End	Specifies the high end inclusive range of TCP/UDP source port numbers to which a packet compares.
IP Dest Port Start	Specifies the low end inclusive range of TCP/UDP destination port number to which a packet compares.

Table 20-16 Details Window Parameters (continued)

Parameter	Description
IP Dest Port End	Specifies the low end inclusive range of TCP/UDP destination port numbers to which a packet compares.
Dest MAC Addr	Indicates the destination MAC address. An Ethernet packet matches an entry when the destination MAC address equals the destination MAC mask.
Dest MAC Mask	Indicates the destination MAC mask. An Ethernet packet matches an entry when the destination MAC address equals the value of the destination MAC mask.
Src MAC Addr	Indicates the source MAC address. An Ethernet packet matches an entry when the source MAC address equals the value of this parameter.
Enet Protocol Type	Indicates the format of the Layer 3 protocol identifier in the Ethernet packet. The options are:
none	Rule does not use the Layer 3 protocol type as a matching criteria.
ethertype	Rule applies only to frames that contain an Ethertype value.
dsap	Rule applies to frames using IEEE802.3 encapsulation format with a Destination Service Access Point (DSAP).
mac	Rule applies to MAC management messages.
all	Rule applies to all Ethernet packets.
Enet Protocol	Indicates the packet class Ethernet protocol. The options are:
none	Parameter is ignored when considering whether a packet matches the current rule.
ethertype	Indicates the 16-bit value of the Ethertype that the packet must match to match the rule.
dsap	Lower 8-bits of the value must match the DSAP byte of the packet to match the rule.
mac	Indicates the lower and upper 8-bits of this object represent the upper and lower bound of MAC management messages.
User Priority Low	Applies to Ethernet frames using the 802.1P/Q tag header. Tagged Ethernet packets must have a 3-bit priority field within the range of the low and high priority to match this rule.

Table 20-16 Details Window Parameters (continued)

Parameter	Description
User Priority High	Applies to Ethernet frames using the 802.1P/Qtag header. Tagged Ethernet packets must have a 3-bit priority field within the range of the low and high priority to match this rule.
VLAN Id	Applies to Ethernet frames using the 802.1P/Qtag header. If this parameter is a non-zero value, tagged packets must have a VLAN identifier that matches the value to match the rule.
State	Indicates whether or not the classifier is currently classifying packets to a Service Flow. The options are: active or inactive.
Packets	Indicates the number of packets that have been classified.
Bit Map	Indicates what parameter encoding were actually present in the DOCSIS packet classifier encoding in the DOCSIS message that created the classifier.

Viewing a Payload Header Suppression Rule

A payload header suppression rule provides the details on how the header bytes of a packet PDU can be omitted and replaced with a payload header suppression index for transmission and subsequently regenerated at the receiving end. The classifier matching a packet may associate with a payload suppression rule.

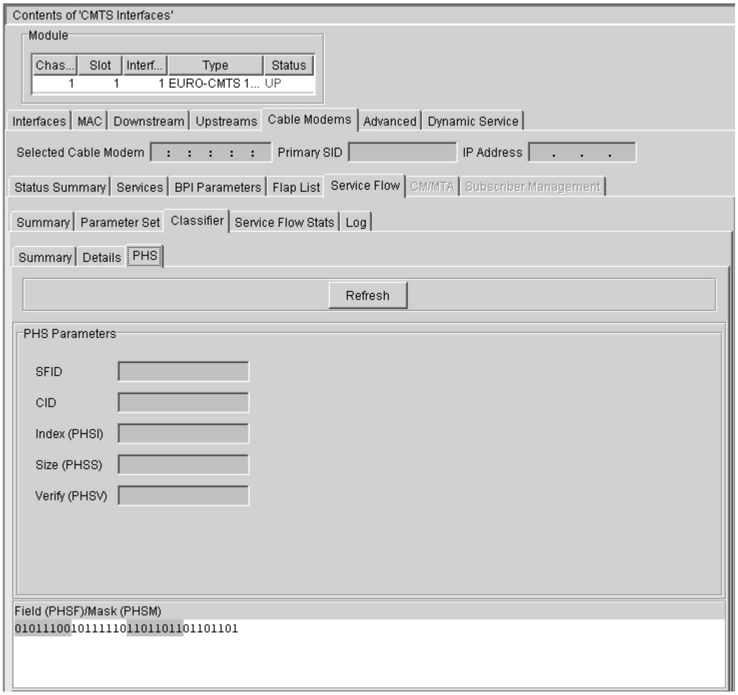
If you delete a Service Flow, you must also delete all classifiers and associated payload suppression rules.

To view a payload header suppression rule, follow this procedure:

1. In the **Summary** window, select the flow that you wish to configure. Refer to Table 20-12.
2. Click the **Classifier** tab. The **Classifier** window appears.
3. Click the **PHS** tab. The **PHS** window appears. Refer to Table 20-17.
4. Click **Refresh** to update the information.

What You See

This figure shows an example of the **PHS** window.



Chas...	Slot	Interf...	Type	Status
1	1	1	EURO-CMTS 1...	UP

Field (PHSF)/Mask (PHSM)

```
01011100101111101101101101101101
```

Parameter Descriptions

This table provides a description of the **PHS** window.

Table 20-17 PHS Window Parameters

Parameter	Description
SFID	Index for a Service Flow that the CMTS assigns.
CID	Index for the service class.
Mask (PHSM)	Defines the bit mask and when combined with the Field parameter, defines which bytes in the header must be suppressed/restored by the sending or receiving device. A bit value of one indicates the byte should be suppressed by the sending device and restored by the receiving device. A bit value of zero indicates the byte should not be suppressed by the sending device or restored by the receiving device.

Table 20-17 PHS Window Parameters (continued)

Parameter	Description
Size (PHSS)	Number of bytes in the heater to be suppressed and restored.
Verify (PHSM)	Payload header suppression verification value. If true, the sender must verify that the Field parameter is the same as what is contained in the packet to be suppressed.
Index	Unique index for the PHS rule on a given Service Flow.
Field	Defines the bytes of the header that must be suppressed/restored by the sending/receiving device.
Mask	Defines the bit mask and when combined with the Field parameter, defines which bytes in the header must be suppressed/restored by the sending or receiving device. A bit value of one indicates the byte should be suppressed by the sending device and restored by the receiving device. A bit value of zero indicates the byte should not be suppressed by the sending device or restored by the receiving device.

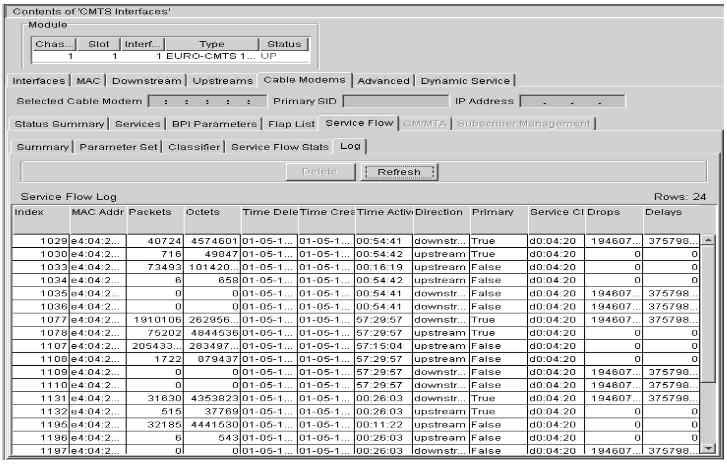
Viewing the Service Flows Log

To view the Service Flow log, follow this procedure:

1. In the **Summary** window, select the flow for which you wish to configure QoS. Refer to Table 20-12.
2. Click the **Log** tab. The **Log** window appears. Refer to Table 20-18.
3. Click **Refresh** to update the information.

What You See

This figure shows an example of the **Log** window.



Chas...	Slot	Interf...	Type	Status
1	1	1	EURO-CMTS 1...	UP

Service Flow Log

Rows: 24

Index	MAC Addr	Packets	Octets	Time Dele	Time Crea	Time Activ	Direction	Primary	Service Cl	Drops	Delays
1029	e4:04:2...	40724	4574601	01-05-1...	01-05-1...	00:54:41	downstr...	True	d0:04:20	194607...	375798...
1030	e4:04:2...	716	49847	01-05-1...	01-05-1...	00:54:42	upstream	True	d0:04:20	0	0
1033	e4:04:2...	73493	101420...	01-05-1...	01-05-1...	00:16:19	upstream	False	d0:04:20	0	0
1034	e4:04:2...	6	658	01-05-1...	01-05-1...	00:54:42	upstream	False	d0:04:20	0	0
1035	e4:04:2...	0	0	01-05-1...	01-05-1...	00:54:41	downstr...	False	d0:04:20	194607...	375798...
1036	e4:04:2...	0	0	01-05-1...	01-05-1...	00:54:41	downstr...	False	d0:04:20	194607...	375798...
1077	e4:04:2...	1910106	262956...	01-05-1...	01-05-1...	57:29:57	downstr...	True	d0:04:20	194607...	375798...
1078	e4:04:2...	75202	4844536	01-05-1...	01-05-1...	57:29:57	upstream	True	d0:04:20	0	0
1107	e4:04:2...	205433...	283497...	01-05-1...	01-05-1...	57:15:04	upstream	False	d0:04:20	0	0
1108	e4:04:2...	1722	879437	01-05-1...	01-05-1...	57:29:57	upstream	False	d0:04:20	0	0
1109	e4:04:2...	0	0	01-05-1...	01-05-1...	57:29:57	downstr...	False	d0:04:20	194607...	375798...
1110	e4:04:2...	0	0	01-05-1...	01-05-1...	57:29:57	downstr...	False	d0:04:20	194607...	375798...
1131	e4:04:2...	31630	4353823	01-05-1...	01-05-1...	00:26:03	downstr...	True	d0:04:20	194607...	375798...
1132	e4:04:2...	515	37769	01-05-1...	01-05-1...	00:26:03	upstream	True	d0:04:20	0	0
1195	e4:04:2...	32185	4441530	01-05-1...	01-05-1...	00:11:22	upstream	False	d0:04:20	0	0
1196	e4:04:2...	6	543	01-05-1...	01-05-1...	00:26:03	upstream	False	d0:04:20	0	0
1197	e4:04:2...	0	0	01-05-1...	01-05-1...	00:26:03	downstr...	False	d0:04:20	194607...	375798...

Parameter Descriptions

This table provides a description of the **Log** window.

Table 20-18 Log Window Parameters

Parameter	Description
Index	Unique index for a logged Service Flow.
Mac Addr	MAC address for the cable modem that associates with the Service Flow.
Packets	Number of packets on this Service Flow after payload header suppression.
Octets	Number of octets on this Service Flow after payload header suppression.
Time Deleted	Time the Service Flow was deleted.
Time Creation	Creation time for the Service Flow.
Time Activation	Total time the flow is active.
Direction	Direction of the Service Flow.
Primary	Indicates whether the Service Flow is the primary or secondary Service Flow.
Service Class Name	Name the CMTS associates with a QoS parameter set.
Drops	Number of packets the flow drops because of policing of the Service Flow, especially to limit the maximum rate of the flow.

Table 20-18 Log Window Parameters (continued)

Parameter	Description
Delays	Number of packets delayed because of policing of the Service Flow, especially to limit the maximum rate of the flow.

Deleting Service Flow Logs

To delete the Service Flow log, follow this procedure:

1. In the **Summary** window, select the flow that you wish to configure. Refer to Table 20-12.
2. Click the **Log** tab. The **Log** window appears. Refer to Table 20-18.
3. Select the Service Flow you wish to delete.
4. Click **Delete**. A confirmation window appears.
5. Click **Ok** to continue with the deletion or click **Cancel**.
6. Click **Refresh** to update the information.

21 CONFIGURING SUBSCRIBER MANAGEMENT

The Cuda 12000, through Subscriber Management, provides added security to your cable network against malicious tampering with the cable modem software, and against unwanted traffic from entering the cable network. Added security is achieved by providing protocol filtering to and from the cable modem, and by limiting the number of IP addresses available to Customer Premise Equipment (CPE) devices.

This section describes Subscriber Management filtering and the following configuration functions:

- Viewing Subscriber Management Summary
- Viewing CPEs Settings
- Configuring CPEs for Subscriber Management
- Assigning Subscriber Management Default Filters
- Configuring Global Subscriber Management Filter Groups

*The Cuda 12000 conforms with the **DOCSIS 1.1 IETF Subscriber Management MIB.***

About Subscriber Management Filtering

Subscriber Management filtering on the Cuda 12000 requires the following configuration procedures:

1. You configure global Subscriber Management filter groups. Global filter groups contain the matching criteria for cable modem packet filters and for CPE devices. Global filter groups apply across the Cuda 12000 and are persisted on the Router Server.
2. You use global filter groups to assign default filter groups for use by cable modems and CPE devices in filtering upstream and downstream traffic

3. During initialization, the cable modem is assigned a Subscriber Management filter group from the provisioning server. (*For information about Subscriber Management configuration on the provisioning server, refer to the* ***FastFlow Broadband Provisioning Manager Guide****, or the guide for your external provisioning manager vendor.)*
4. If Subscriber Management filter groups do not exist on the provisioning server, the cable modem is assigned a default filter group on the Cuda 12000.
5. If the network administrator chooses not to use the criteria of the global filter group for a particular cable modem, the administrator may modify the global filter group. Modifications to filter groups on a per cable modem basis are temporary assignments and available only for the current session. The modifications do not persist, so the original filter group is not overwritten.

How Filtering Works

The IP packet filtering system and Subscriber Management filter operate in serial. The packet is dropped if either filter denies the packet; for example:

- If your network is configured to use both the IP packet and Subscriber Management filters, the packet is first filtered through the IP packet matching criteria.
- If the IP packet denies the packet, the packet is dropped and is not forwarded.
- If the packet is accepted by the IP packet, the packet is filtered through the Subscriber Management filter.
- If the Subscriber Management filter denies the packet, the packet is dropped.
- If the packet is accepted by the Subscriber Management filter, the packet is forwarded.

For detailed information on IP packet filters, refer to Chapter 14, “IP Packet Filtering”.

Before You Begin

Before you configure subscriber management, follow this procedure:

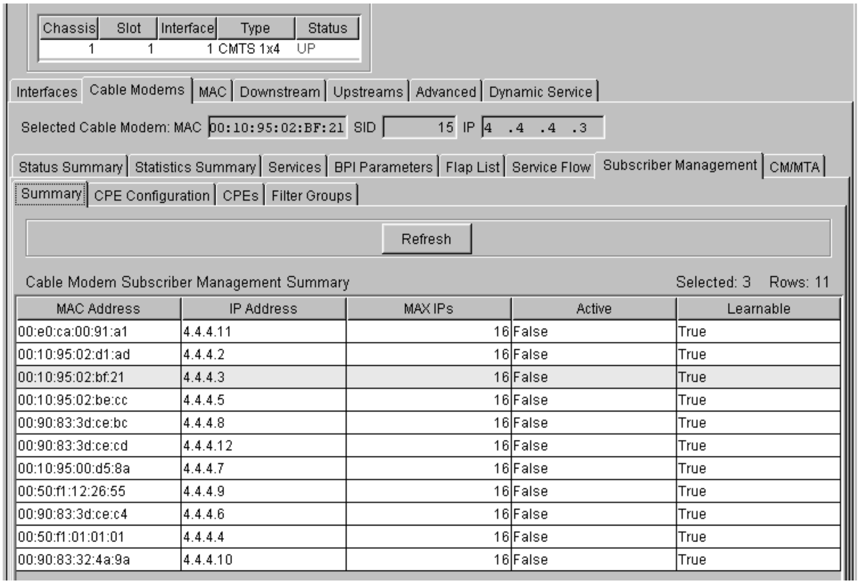
1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **CMTS** > **Interfaces**
2. Click **Cable Modems** tab.
3. Click **Subscriber Management** tab. The Cable Modem Subscriber Management Summary window appears.

Viewing Subscriber Management Summary

The Cable Modem Subscriber Management Summary window displays the state of subscriber management on cable modems.

What You See

Figure 21-1 Subscriber Management Summary Window



Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

Selected Cable Modem: MAC 00:10:95:02:BF:21 SID 15 IP 4 .4 .4 .3

Cable Modem Subscriber Management Summary Selected: 3 Rows: 11

MAC Address	IP Address	MAX IPs	Active	Learnable
00:e0:ca:00:91:a1	4.4.4.11	16	False	True
00:10:95:02:d1:ad	4.4.4.2	16	False	True
00:10:95:02:bf:21	4.4.4.3	16	False	True
00:10:95:02:be:cc	4.4.4.5	16	False	True
00:90:83:3d:ce:bc	4.4.4.8	16	False	True
00:90:83:3d:ce:cd	4.4.4.12	16	False	True
00:10:95:00:d5:8a	4.4.4.7	16	False	True
00:50:f1:12:26:55	4.4.4.9	16	False	True
00:90:83:3d:ce:c4	4.4.4.6	16	False	True
00:50:f1:01:01:01	4.4.4.4	16	False	True
00:90:83:32:4a:9a	4.4.4.10	16	False	True

Parameter Descriptions

This table provides a description of the Summary window

Table 21-1 Cable Modem Subscriber Management Summary Window Parameters:

Parameter	Description
MAC Address	MAC address of the cable modem.
IP Address	IP address of the attached cable modem.
MAX IPs	Number of simultaneous CPE IP addresses you can attach to the cable modem. If this parameter is set to zero, the cable modem drops all CPE traffic. This value is invalid if the **Active** parameter is set to False. Allowable range is 0 to 16.
Active	Indicates the status of subscriber management. The options are:
True	CMTS based CPE control is active and all actions required by the various filter tables and controls apply at the CMTS.
False	No subscriber filtering is applied at the CMTS. This is the default.

Parameter	Description
Learnable	Indicates if the ability to learn IP addresses is enabled or disabled.
True	CMTS can learn CPE IP addresses up to the value configured in the MAX IP parameter. This is the default.
False	CMTS does not learn CPE IP addresses.

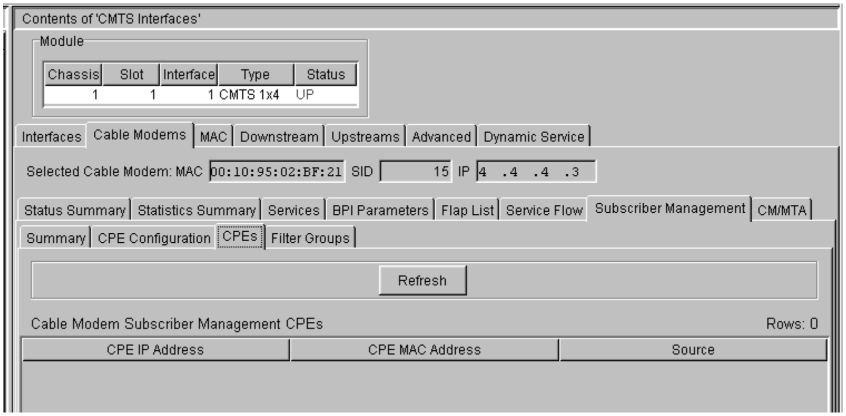
Viewing CPEs Settings

To view summary information for cable modem subscriber management for CPEs, follow this procedure:

1. From the Summary window (Figure 21-1, “Subscriber Management Summary Window”), select the cable modem for which you wish to view the CPE information.
2. Click the **CPEs** tab. The CPE window appears.
3. Click Refresh to update the window.

What You See

Figure 21-2 CPE Summary Window



Contents of 'CMTS Interfaces'

Module

Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

Selected Cable Modem: MAC 00:10:95:02:BF:21 SID 15 IP 4 .4 .4 .3

Cable Modem Subscriber Management CPEs Rows: 0

CPE IP Address	CPE MAC Address	Source

Parameter Descriptions

CPE Summary Window parameters

Table 21-2 :CPE Summary Window Parameter Descriptions

Parameter	Description
CPE IP Address	IP address for the attached CPE.
CPE MAC Address	The MAC address of the cable modem behind which the CPE device is attached.
Source	Indicates how the entry was created. The options are: ■ manual ■ learned ■ other

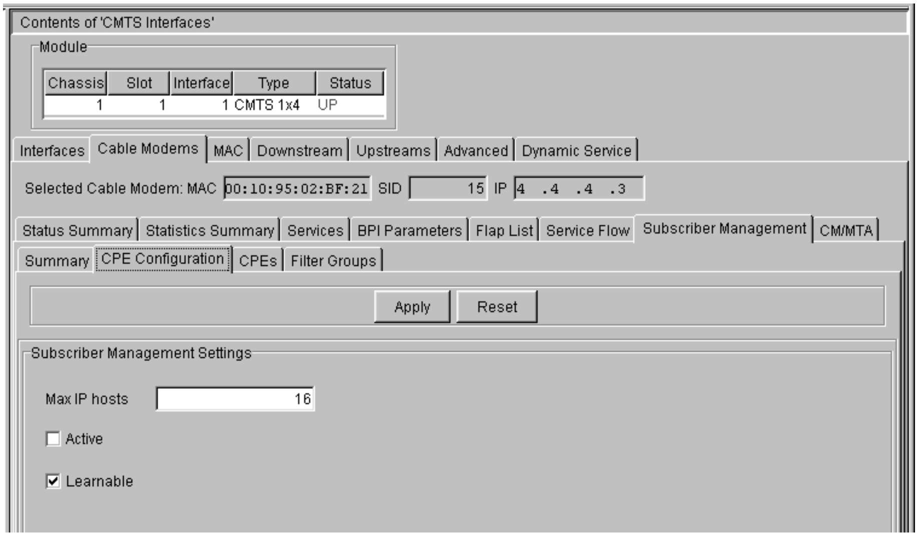
Configuring CPEs for Subscriber Management

To configure the default information for a cable modem, follow this procedure:

1. From the Cable Modem Subscriber Management Summary window, select the row that includes the MAC address of the cable modem behind which the specific CPE is attached.
2. Click the **CPE Configuration** tab. The Subscriber Management Settings window appears.
3. Enter values for the parameters. Refer to Table 21-3.
4. Click **Apply** to commit the information or click **Reset** to return to the default values.

What You See

Figure 21-3 CPE Subscriber Management Settings Window



Contents of 'CMTS Interfaces'

Module

Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

Selected Cable Modem: MAC 00:10:95:02:BF:21 SID 15 IP 4 .4 .4 .3

Subscriber Management Settings

Max IP hosts 16

□ Active

☑ Learnable

Parameter Descriptions

This table provides a description of the CPE Configuration window parameters:

Table 21-3 Subscriber Management Settings Window Parameters

Parameter	Description
Max IP hosts	Number of simultaneous CPE IP addresses you can attach to the cable modem. If this parameter is set to zero, the cable modem drops all CPE traffic. This value is invalid if the **Active** parameter is set to False. By default, Max IP hosts is set to 16. Allowable values are 1 to 16.
Active	Indicates the status of subscriber management. If the check box is enabled, the CMTS-based CPE control is active and all actions required by the various filter tables and controls apply at the CMTS. If the check box is cleared, no subscriber filtering is applied at the CMTS.

Parameter	Description
Learnable	Indicates if the ability to learn IP addresses is enabled or disabled. If the check box is enabled, the CMTS can learns CPE IP addresses up to the value configured in the MAX IP parameter. If the check box is cleared, the CMTS does not learn CPE IP addresses.

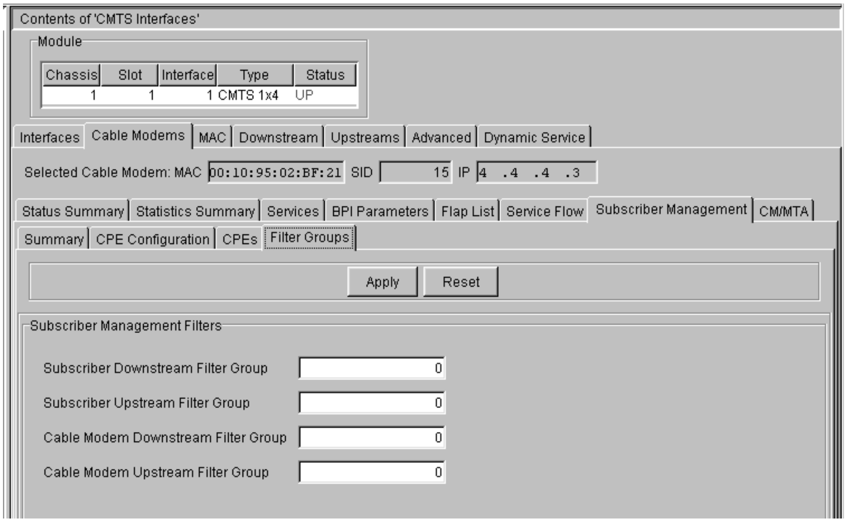
Assigning Subscriber Management Default Filters

To assign subscriber management default filters, follow this procedure:

1. From the Cable Modem Subscriber Management Summary window, select the row that includes the MAC address of the cable modem behind which the specific CPE is attached.
2. Click the **Filter Groups** tab. The Subscriber Management Filters window appears.
3. Enter values for the parameters. Refer to Table 21-4.
4. Click **Apply** to commit the changes or **Reset** to return the window to the default values.

What You See

Figure 21-4 Subscriber Management Filters Window



Contents of 'CMTS Interfaces'

Module

Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

Selected Cable Modem: MAC 00:10:95:02:BF:21 SID 15 IP 4 .4 .4 .3

Subscriber Management Filters

Subscriber Downstream Filter Group	0
Subscriber Upstream Filter Group	0
Cable Modem Downstream Filter Group	0
Cable Modem Upstream Filter Group	0

Parameter Descriptions

This table provides a description of the Filters window:

Table 21-4 Subscriber Management Filters Window Parameters:

Parameter	Description
Subscriber Downstream Filter Group	The ID of the filter group that you specify to be the default filter group, to be used by CPE devices for downstream traffic.
Subscriber Upstream Filter Group	The ID of the filter group that you specify to be the default filter group, to be used by CPE devices for upstream traffic.
Cable Modem Downstream Filter Group	The ID of the filter group that you specify to be the default filter group, to be used by cable modems for downstream traffic.
Cable Modem Upstream Filter Group	The ID of the filter group that you specify to be the default filter group, to be used by cable modems for upstream traffic.

Configuring Global Subscriber Management Filter Groups

Configuring global filter groups on the Cuda 12000 involves defining the matching criteria to be used globally across the Cuda 12000.

You can configure up to 60 global filter groups. Each filter group may contain up to 40 matching criteria rules.

Before you configure the matching criteria for global Subscriber Management filter groups, bear in mind that you may use Subscriber Management filter groups in addition to the IP packet filtering system, which is the default on the Cuda 12000.

Before You Begin

Before you begin to configure the cable modem packet filters and groups, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > **Cuda Chassis Manager** > **Configuration** > **IP** > **CM Packet Filters**.
2. The Summary window appears.

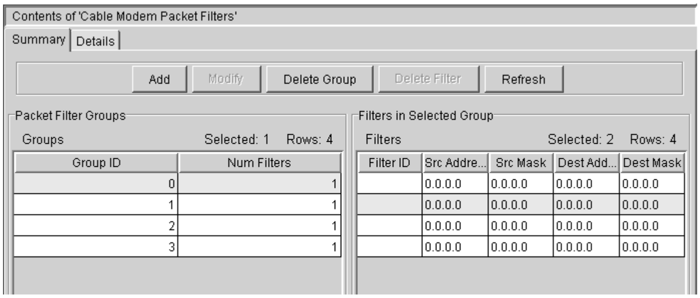
Viewing Packet Filter Groups

You can view the current packet filters for all cable modems. To view the cable modem packet filters, follow this procedure:

1. From the Summary window, select the Group ID for the filters you wish to view. The filters for that selected group appears in the adjacent table.
2. Click **Refresh** to update the window information.

What You See

Figure 21-5 Summary window.



Contents of 'Cable Modem Packet Filters'

Packet Filter Groups

Groups Selected: 1 Rows: 4

Group ID	Num Filters
0	1
1	1
2	1
3	1

Filters in Selected Group

Filters Selected: 2 Rows: 4

Filter ID	Src Addre...	Src Mask	Dest Add...	Dest Mask
	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0

Parameter Descriptions

The following table lists the matching criteria parameters that you configure to create global Subscriber Management filter groups on the Cuda 12000.

Table 21-5 Summary Window Parameters

Parameter	Description
Packet Filter Groups	
Group ID	Identifies the ID for the set of filters specifications. You can associate a cable modem and CPE device with a filter group for its upstream traffic and a filter group for its downstream traffic. A cable modem and CPE device can also use the same filter group for upstream and downstream within the group. Allowable values range from 1 to 60.
Num Filters	Number of filters located in a group. Allowable values range from 1 to 40.
Filters in Selected Groups	
Filter ID	Identifies the ID for the filter within the selected group.

Parameter	Description
Src Address	Source IP address. The filter attempts to match the source IP address to the IP address in the IP packet. If the addresses match, the filter is applied to the packet.
Src Mask	Bit mask that applies to the source IP address prior to matching. The source IP address and mask are the matching criteria for the packet. By default, the source IP address and mask specify a filter that matches all source addresses. This mask entry is not necessarily the same as the subnet mask.
Dest Add	Destination IP address. The filter attempts to match the destination IP address to the IP address in the IP packet. If the addresses match, the filter is applied to the packet.
Dest Mask	Bit mask that applies to the destination address prior to matching. The destination IP address and mask are the matching criteria for the packet. By default, the destination IP address and mask specify a filter that matches all destination addresses. The mask entry is not necessarily the same as the subnet mask.

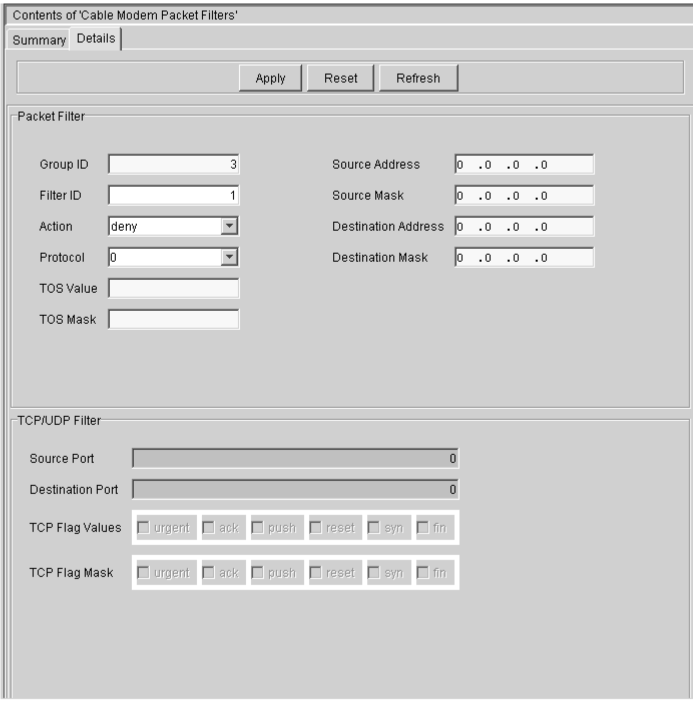
Adding a Packet Filter Group

To add a packet filter group, follow this procedure:

1. From the Summary window, click **Add**. The Details window appears.
2. Enter values for the parameters. Refer to Table 21-6.
3. Click **Apply** to commit the change or click **Reset** to return the values to the default.
4. Click **Refresh** to update the information.

What You See

Figure 21-6 Details window.



Group ID: 3
Filter ID: 1
Action: deny
Protocol: 0
TOS Value:
TOS Mask:
Source Address: 0 .0 .0 .0
Source Mask: 0 .0 .0 .0
Destination Address: 0 .0 .0 .0
Destination Mask: 0 .0 .0 .0

Source Port: 0
Destination Port: 0
TCP Flag Values: □ urgent □ ack □ push □ reset □ syn □ fin
TCP Flag Mask: □ urgent □ ack □ push □ reset □ syn □ fin

Parameter Descriptions

This table provides a description of the Details window packet filter parameters.

Table 21-6 Cable Modem Packet Filter Group Details Window

Parameter	Description
Group ID	Group number specifies the ID of the filter group to which you want the filter to belong. Allowable values range from 1 to 60.
Filter ID	Filter number specifies the index number for the filter within the group. Allowable values range from 1 to 40.
Action	Action to take upon this filter matching. The options are:
Permit	Forward the packet for further processing. The default is to permit the packet.
Deny	Drop the packet.
Protocol	The protocol that the filter attempts to match. Specify one of the following protocols: TCP, UDP, Any, and Number. ■ You may obtain protocol numbers from the Internet Assigned Numbers Authority (IANA) at www.iana.org. ■ You may specify a protocol number from 0 to 256. Note that specifying 256 is the same as specifying "Any."
TOS Value	The two-digit hexadecimal number indicating the Type of Service (ToS) value to be matched against the ToS value in IP packets (for example, 0a). The default is 00.
TOS Mask	The two-digit hexadecimal number that specifies the mask to be applied to the TOS value matched in the IP packet (for example 1b). The mask determines which bits are matched (a 0 specifies a match while a 1 specifies no match). The default is 00, which means that the ToS value you specify is matched against all TOS values in IP packets.
Src Address	The filter attempts to match the source IP address to the IP address in the IP packet. If the addresses match, the filter is applied to the packet.
Src Mask	Bit mask that applies to the source IP address prior to matching. The source IP address and mask are the matching criteria for the packet. By default, the source IP address and mask specify a filter that matches all source addresses. This mask entry is not necessarily the same as the subnet mask.
Dest Add	The filter attempts to match the destination IP address to the IP address in the IP packet. If the addresses match, the filter is applied to the packet.

Parameter	Description
Dest Mask	Bit mask that applies to the destination IP address prior to matching. The destination IP address and mask are the matching criteria for the packet. By default, the destination IP address and mask specify a filter that matches all destination addresses. The mask entry is not necessarily the same as the subnet mask.
TCP/UDP Filter	
Source Port (Applies only to TCP or UDP filters.)	Optional. The source TCP or UDP port number to match. Specify one of the following values: ■ Any: Match any source port ■ Number: Match a source port number to the TCP or UDP port. The allowable TCP or UDP port number range is 0 to 65536. Note that specifying 65536 is the same as specifying “Any.”
Destination Port (Applies only to TCP or UDP filters.)	Optional. The destination TCP or UDP port number to match. Specify one of the following values: ■ Any: Match any source port ■ Number: Match a source port number to a TCP or UDP port. The allowable TCP or UDP port number range is 0 to 65536. Note that specifying 65536 is the same as specifying “Any.”
TCP Flag Values	Optional. The value of the TCP flags. The following is a list of the TCP flag options. Leaving this field blank indicates a null value (no flags). TCP flags must always be a subset of the TCP flag mask in order for the packet header to be matched. ■ For example, to match all packets where only the “urgent” flag is set, and the mask is set at “syn”, and “fin,” the resulting flag values would be “urgent” and the mask would be: “urgent, syn, fin.”
urgent	Indicates the TCP segment is urgent
ack	Indicates the acknowledgement number field in the TCP field segment is significant.
push	Indicates the TCP software to push all the data sent so far through the pipeline to the receiving application.
reset	Indicates the connection is reset.
syn	Indicates that the sequence numbers are resynchronized, marking the beginning of a connection.

Parameter	Description
fin	Indicate the transmitting CPE has no more data to transmit.
TCP Flag Mask	Optional. The flag of interest in the TCP header for the packet to match. Leaving this field blank indicates a null value (no flags)
urgent	Indicates the TCP segment is urgent
ack	Indicates the acknowledgement number field in the TCP field segment is significant.
push	Indicates the TCP software to push all the data sent so far through the pipeline to the receiving application.
reset	Indicates the connection is reset.
syn	Indicates that the sequence numbers are resynchronized, marking the beginning of a connection.
fin	Indicate the transmitting CPE has no more data to transmit.

Modifying Packet Filter Groups

Follow this procedure to modify a packet filter group:

1. In the Summary window, select the filter you wish to modify and click **Modify Filter**. The Details window appears. Refer to Figure 21-6.
2. Update the information. Refer to Table 21-6.
3. Click **Apply** to commit the changes or click **Reset** to return to previous values.
4. Click **Refresh** to update the window information.

Deleting Packet Filter Groups

Follow this procedure to delete packet filter groups:

1. In the Summary window, select the group that includes the filter you wish to delete from the Packet Filter Groups table. The filters for that group appear in the Filters in Selected Group table. Refer to Figure 21-6.
2. From the Filters in Selected Groups table, select the filter you wish to delete.
3. Click **Delete Filter**. A confirmation window appears.
4. Click **Ok** to delete the group or select **Cancel** to cancel the deletion.
5. Click **Refresh** to update the information.

22 BROWSING MIBS

The Cuda 12000 supports MIB browsing of cable modems and embedded Multimedia Terminal Adapters (MTAs). This chapter provides information on how to browse cable modem and MTA MIBs, and the MIB objects that are returned.

The cable modem and MTA MIB tables are in compliance with *DOCSIS Operations Support System Interface Specification SP-OSSIv1.1-103-001220; DOCSIS Baseline Privacy Plus Interface Specification SP-BPI+-106001215*; *PacketCable Security Specification PKT-SP-SEC_I02-001229*; RFC2669, RFC2670, and RFC3083.

Cable Modem MIBs

The following is a list and description of the cable modem MIB tables that are supported by the Cuda 12000:

Table 22-1 Cable Modem MIB Tables

MIB Table	Description
docsIfCmMacTable	Describes the attributes of each cable modem MAC interface.
docsIfCmServiceTable	Describes the attributes of each upstream service queue.
docsIfCmStatusTable	Maintains status objects and counters for cable modems.
docsIfDownstreamChannelTable	Describes the attributes of the downstream channel.
docsIfUpstreamChannelTable	Describes the attributes of attached upstream channels. This table is implemented on both the CMTS and cable modem.
docsIfSignalQualityTable	Describes PHY signal quality for downstream channels.
docsIfQosProfileTable	Describes the attributes for each class of service.
docsBpiCmBaseTable	Describes the basic- and authorization-related Baseline Privacy attributes of each cable modem MAC interface
docsBpiCmTEKTable	Describes the attributes of each CM Traffic Encryption Key (TEK) association. The CM maintains (no more than) one TEK association per SID per CM MAC interface.
docsBpi2CmBaseTable	Describes the basic- and authorization-related Baseline Privacy Plus attributes of each cable modem MAC interface.
docsBpi2CmTEKTable	Describes the attributes of each CM Traffic Encryption Key (TEK) association for BPI Plus.
systemGroup	Provides system identification, such as, contact name, device name and location.

MIB Table	Description
subset of ifTable & ifXTable	Provides status information and statistics on interface activity.
docsDevBaseGroup, docsDevSoftwareGroup, docsDevServerGroup	Provides objects needed for cable device system management.
docsDevEvControl	Provides control and logging for event reporting, and contains the following MIB tables: ■ docsDevEvSyslog ■ docsDevEvThrottleAdminStatus ■ docsDevEvThrottleInhibited ■ docsDevEvThrottleThreshold ■ docsDevEvThrottleInterval

MTA MIBs

The following is a list and description of the MTA MIB tables that are supported by the Cuda 12000:

Table 22-2 MTA MIB Tables

MIB Table	Description
pktcMtaDevBase	Provide general information regarding the MTA device for the particular interface.
pktcMtaDevServer	Provides the information that the MTA device uses to initialize when it boots up.
pktcMtaDevSecurity	Provides the public key certificates and other security-related information for the MTA device.
pktcSigDevConfigObjects, pktcSigDevCodecTable, pktcSigEndPntConfigTable	Contains information regarding Display Network Call Signaling (NCS). NCS displays include values for the following parameters. ▪ Service-level Configuration ▪ CODEC Conversion Types ▪ End Point IDs

Browsing Cable Modem and MTA Status

The Cuda 12000 supports the retrieval and display of status information that is maintained by individual cable modems and MTAs connected to the HFC network. This information is useful when you have to monitor the network and troubleshoot network problems.

To retrieve and display this status information:

1. Navigate to **Network Browser** > GroupName > ChassisName > C**uda Chassis Manager** > **Configuration** > **CMTS** > **Interfaces**.
2. Click the **Cable Modems** tab.
3. Click the **CM/MTA** tab.

Table 22-3 Tabs for Accessing Cable Modem and MTA MIB Tables

Tab Name	MIB Table or Group
CM Status	CM Status (docsIfCMStatusTable). Refer to Table 22-6 on page 633.
CM MAC	CM MAC (docsIfCmMacTable). Refer to Table 22-4 on page 632.
CM Service	CM Service (docsIfCMServiceTable). Refer to Table 22-5 on page 632.
Downstream	Downstream (docsIfDownstreamChannelTable). Refer to Table 22-7 on page 634.
Upstream	Upstream (docsIfUpstreamChannelTable). Refer to Table 22-8 on page 635.
Signa Quality	Signal Quality (docsIfSignalQualityTable). Refer to Table 22-9 on page 636.
QoS	QOS (docsIfQosProfileTable). Refer to Table 22-10 on page 637.
BPI > BPI Base	BPI Base (docsBPICMBaseTable). Refer to Table 22-11 on page 638.
BPI > BPI TEK	BPI TEK (docsBPICMTEKTable). Refer to Table 22-12 on page 642.
BPI > BPI Plus Base	BPI Plus Base (docsBpi2CmBaseTable). Refer to Table 22-13 on page 644.
BPI > BPI Plus TEK	BPI Plus TEK (docsBPI2CmTEKTable). Refer to Table 22-14 on page 649.

Tab Name	MIB Table or Group
System	System (systemGroupTable). Refer to Table 22-15 on page 651.
Device > **Device Configuration**	Device (docsDevBase, docsDevSoftware, docsDevServer). Refer to Table 22-16 on page 651.
Device > **Event Configuration**	Device Event Configuration (docsDevEvControlTable). Refer to Table 22-17 on page 654.
Device > **Events**	Device Event List (docsDevEventTable). Refer to Table 22-18 on page 655.
Device > **Event Control**	Device Event Control (docsDevEvControlTable). Refer to Table 22-19 on page 656.
Interfaces	Interface (ifTable and ifXTable). Refer to Table 22-20 on page 657.
MTA > **Base**	MTA Base (pktcMtaDevBaseTable). Refer to Table 22-21 on page 659.
MTA > **Server**	MTA Server (pktcMtaDevServerTable). Refer to Table 22-22 on page 660.
MTA > **Security**	MTA Security (pktcMtaDevSecurityTable).
MTA > **NCS** > **Configuration**	MTA Signalling Configuration (pktcSigDevConfigObjects). Refer to Table 22-25 on page 662.
MTA > **NCS** > **Codec**	MTA Codec (pktcSigDevCodecTable). Refer to Table 22-24 on page 661.
MTA > **NCS** > **End Points**	MTA Endpoint (pktcSigEndPntConfigTable). Refer to Table 22-23 on page 661.

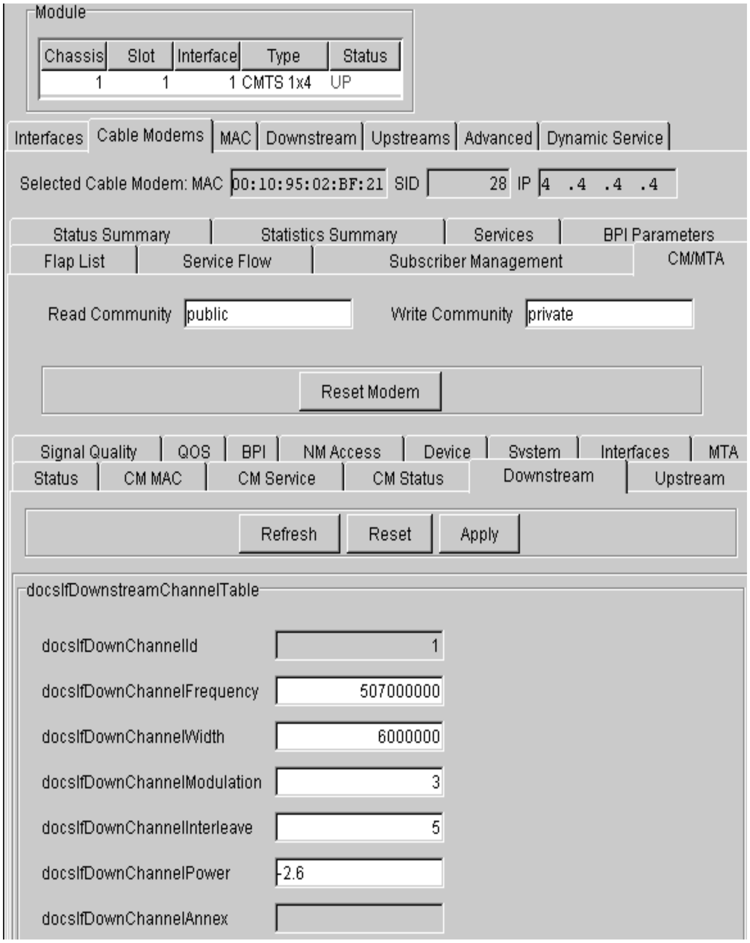
Example

For example, to display cable modem downstream status, follow this procedure:

1. Navigate to **Network Browser** > GroupName > ChassisName > C**uda Chassis Manager** > **Configuration** > **CMTS** > **Interfaces**.
2. Click the **Cable Modems** tab.
3. Click the **CM/MTA** tab.
4. Click the **Downstream** tab.

The corresponding output from the cable modem’s MIB would be:

Figure 6-1 CM/MTA Downstream MIB Window



Module

Chassis	Slot	Interface	Type	Status
1	1	1	CMTS 1x4	UP

Selected Cable Modem: MAC 00:10:95:02:BF:21 SID 28 IP 4 .4 .4 .4

Read Community public

Write Community private

docsIfDownstreamChannelTable

docsIfDownChannelId	1
docsIfDownChannelFrequency	507000000
docsIfDownChannelWidth	6000000
docsIfDownChannelModulation	3
docsIfDownChannelInterleave	5
docsIfDownChannelPower	-2.6
docsIfDownChannelAnnex	

Cable Modem and MTA Output Descriptions

Table 22-4 CM MAC Parameters

Field Output	Description
docsIfCmCmtsAddress	MAC address of the CMTS that is believed to control this MAC domain. At the cable modem, this the source address from the SYNC, MAP, and other MAC-layer messages. If the CMTS is unknown, this value is 00-00-00-00-00-00.
docsIfCmCapabilites	Capabilities of the MAC implementation at this interface.
docsIfCmRangingRespTimeout	Waiting time for a ranging response packet.
docsIfCmRangngTimeout	Waiting time for a ranging timeout packet.

Table 22-5 CM Service Parameters

Field Output	Description
docsIfCmServiceQoSProfile	Indicates the QoS attributes that associate with this particular service. A value of zero indicates no associated profile.
docsIfCmServiceTXSlotsImme	Number of upstream mini-slots that were used to transmit data PDUs in immediate contention mode. This includes only PDUs that are presumed to have arrived at the headend. It does not include re-transmission attempts or mini-slots used by Requests.
docsIfCmServiceTx SlotsDed	Number of upstream mini-slots that are used to transmit data PDUs in dedicated mode. For example, as a result of a unicast data grant.
dosIfCmServiceTXRetries	Number of attempts to transmit data PDUs containing requests for acknowledgement that did not result in acknowledgement.
docsIfCmServiceTxExceededs	Number of data PDUs transmission failures due to excessive retries without acknowledgement.
docsIfCmServiceRqRetries	Number of attempts to transmit bandwidth requests that did not result in acknowledgement.

Field Output	Description
docsIfCmServiceRqExceededs	Number of requests for bandwidth that failed due to excessive retries without acknowledgement.

Table 22-6 CM Status Parameters

Field Output	Description
docsIfCmServiceStatusValue	Current cable modem connectivity state.
docsIfCmServiceStatusCode	Status code for this cable modem. This value consists of a single character indicating an error group and two or three numbers indicating the status condition.
docsIfCmServiceTxPower	Operational transmit power for the attached upstream channel.
docsIfCmServiceResets	Number of times the cable modem resets or initializes.
docsIfCmServiceLostSyncs	Number of times the cable modem lost synchronization with the downstream channel.
docsIfCmServiceInvalidMaps	Number of times the cable modem receives invalid MAP messages.
docsIfCmServiceInvalidUcds	Number of times the cable modem receives invalid UCD messages.
docsIfCmServiceInvalidRangi	Number of times the cable modem receives invalid ranging response messages.
docsIfCmServiceInvalidRegis	Number of times the cable modem receives invalid registration response messages.
docsIfCmServiceT1Timeouts	Number of times counter T1 expires in the cable modem.
docsIfCmServiceT2Timeouts	Number of times counter T2 expires in the cable modem.
docsIfCmServiceT3Timeouts	Number of times counter T3 expires in the cable modem.
docsIfCmServiceT4Timeouts	Number of times counter T4 expires in the cable modem.
docsIfCmServiceRangingAbort	Number of times the ranging process was aborted by the CMTS.

Table 22-7 Downstream Parameters

Field Output	Description
docsIfDownChannelID	CMTS identification of the downstream channel within this particular MAC interface. If the interface is down, the most current value displays. If the channel ID is unknown, a value of zero displays.
docsIfDownChannelFrequency	Center of the downstream frequency, in hertz, associated with this channel. This object returns the current tuner frequency. If a CMTS provides IF output, a value of zero displays unless the CMTS is in control of the final downstream RF frequency.
docsIfDownChannelWidth	Bandwidth, in hertz, of this downstream channel.
docsIfDownChannelModulation	Modulation type for this downstream channel. If the interface is down, this object either returns the configured value from the CMTS, the most current value from the cable modem, or a value of unknown. The options are: unknown, other, qam64, or qam256.
docsIfDownChannelInterleave	Forward Error Correction (FEC) interleaving for this downstream channel.
docsIfDownChannelPower	At the CMTS, the operational transmit power. At the cable modem, the received power level. You can set this parameter to zero at the cable modem is power level management is not supported. If the interface is down, the value is either the value configured at the CMTS, the most current value from the cable modem, or a value of zero.
docsIfDownChannelAnnex	*MIB browsing for this field is not supported in this release.*

Table 22-8 Upstream Parameters

Field Output	Description
docsIfUpChannelId	CMTS identification of the upstream channel within this particular MAC interface. If the interface is down, the most current value displays. If the channel ID is unknown, a value of zero displays.
docsIfUpChannelFrequency	Center of the downstream frequency, in hertz, associated with this channel. This object returns a value of zero if the frequency is undefined or unknown,
docsIfUpChannelWidth	Bandwidth, in hertz, of this upstream channel.
docsIfDownChannelModulation Profile	Modulation profile for this upstream channel.
docsIfUpChannelSlotSize	Number of 6.25 microsecond ticks in each upstream mini-slot.
docsIfUpChannelTxTimingOffset	Timing, in units of 6.25 microseconds, of cable modem upstream transmissions to ensure synchronized arrivals at the CMTS. The value indicates the current round trip time at the cable modem or the maximum round trip time seen at the CMTS.
docsIfUpChannelRangingBackoff Start	Initial random backoff window to use when retrying ranging requests. This is expressed as power of 2. For example, a value of 16 at the CMTS indicates that a proprietary adaptive retry mechanism is to be used.
docsIfUpChannelRangingBackoff End	Final random backoff window to use when retrying ranging requests. Expressed as a power of 2. For example, a value of 16 at the CMTS indicates that a proprietary adaptive retry mechanism is to be used.
docsIfUpChannelTxBackoffStart	Initial random backoff window to use when retrying transmissions. This is expressed as power of 2. For example, a value of 16 at the CMTS indicates that a proprietary adaptive retry mechanism is to be used.

Field Output	Description
docsIfUpChannelTxBackoffEnd	Final random backoff window to use when retrying transmissions. Expressed as a power of 2. For example, a value of 16 at the CMTS indicates that a proprietary adaptive retry mechanism is to be used.

Table 22-9 Signal Quality Parameters

Field Output	Description
docsIfSigQIncludes Contention	Indicates the signal includes contention. The options are:
True	CMTS includes contention intervals. A value of 1 indicates True.
False	CMTS does not include contention intervals. This parameter is always False for cable modems. A value of 2 indicates False.
docsIfSigQUnerroreds	Number of codewords this channel receives without error.
docsIfSigQCorrecteds	Number of codewords that this channel receives with correctable errors.
docsIfSigQUncorrectables	Number of codewords this channel received with uncorrectable errors.
docsIfSigQSignalNoise	Signal/Noise ratio, in dB, for this channel. At the cable modem, this is the signal/noise ration of this downstream channel. At the CMTS, this is the average signal/noise of the upstream channel.
docsIfSigQMicroreflections	Total number of microreflections on this interface.
docsIfSigQEqualization Data	At the cable modem, this value indicates the equalization data for the downstream channel. At the CMTS, this value indicates the average equalization data for the upstream channel.

Table 22-10 QOS Parameters

Field Output	Description
docsIfQosProfPriority	Relative priority assigned to this service when allocating bandwidth. Zero indicates lowest priority, and seven indicates the highest priority.
docsIfQosProfMaxUpBandwidth	Maximum upstream bandwidth, in bps, the service allows with this service class.
docsIfQosProfGuarUpBandwidth	Minimum guaranteed upstream bandwidth, in bps, the service allows with this service class.
docsIfQosProfMaxDownBandwidth	Maximum downstream bandwidth, in bps, the service allows with this service class.
docsIfQosProfMaxTxBurst	Maximum number of mini-slots that may be requested for a single upstream transmission. A value of zero indicates no limit.
docsIfQosProfBaselinePrivacy	Indicates whether Baseline Privacy is enabled for this service class.
docsIfQosProfStatus	Creates or deletes rows in the table. You must not change a row while it is active.

Table 22-11 BPI > BPI Base Parameters

Field Output	Description
docsBpiCmPrivacyEnable	Indicates if the cable modem is provisioned to run Baseline Privacy.
docsBpiCmPublicKey	Indicates the DER-encoded RSA public key corresponding to the public key of the cable modem.
docsBpiCmAuthState The options are:	State of the cable modem authorization Finite State Machine (FSM).
Start	FSM is in its initial state.
authwait	The cable modem has received the “Provisioned” event, indicating that it has completed RF MAC registration with the CMTS. In response to receiving the event, the cable modem has sent both an Authentication information and an Authorize Request message to the CMTS and is waiting for the reply.
Authorized	The cable modem has received an Authorization Reply message which contains a list of valid SAIDs for this cable modem. At this point, the modem has a valid Authorization Key and SAID list. Transition into this state triggers the creation of on TEK FSM for each of the cable modem’s privacy-enabled SAIDs.
ReauthWait	The cable modem has an outstanding re-authorization request. The cable modem was either about to time out its current authorization or received an indication (an Authorization Invalid message from the CMTS) that its authorization was no longer valid. The cable modem sent an Authorization Request message to the CMTS and is waiting for a response.

Field Output	Description
Auth Reject Wait	The cable modem received an Authorization Reject message in response to its last Authorization Request. The Authorization Reject's error code indicated that the error was not of a permanent nature. In response to receiving this reject message, the cable modem set a timer and transitioned to the Authorized Reject Wait state. The cable modem remains in this state until the timer expires.
docsBpiCmAuthKeySequence Number	Authorized key sequence number of this FSM.
docsBpiCmAuthExpires	Actual clock time when the current authorization for this FSM expires. If the cable modem does not have an active authorization, the value is the expiration date and time of the last active authorization.
docsBpiCmAuthReset	Determines the reauthorize event status.
The options are:	
True	Generates a reauthorize event in the authorization FSM
False	Does not generate an authorization event.
docsBpiCmAuthGraceTime	Grace time for an authorization key. A cable modem is expected to start trying for a new authorization key beginning the grace time number of seconds before the authorization key actually expires. This value cannot change while the authorization state machine is operating.
docsBpiCmTEKGraceTime	The TEK Grace Time in seconds before TEK expires.
docsBpiCmAuthWaitTimeout	The authorize wait timeout. This value cannot change while the authorization state machine is operating.
docsBpiCmReauthWaitTimeout	Reauthorize wait timeout, in seconds. This value cannot change while the authorization state machine is operating.

Field Output		Description
docsBpiCmOpWaitTimeout		Operational wait timeout, in seconds. This value cannot change while the authorization state machine is operating.
docsBpiCmRekeyWaitTimeout		Rekey wait timeout, in seconds. This value cannot change while the authorization state machine is operating.
docsBpiCmAuthRejectWaitTimeout		Authorization reject wait timeout, in seconds. This value cannot change while the authorization state machine is operating.
docsBpiCmAuthRequests		Number of times the cable modem has transmitted an authorization request message.
docsBpiCmAuthReplies		Number of times the cable modem receives an authorization reply message.
docsBpiCmAuthRejects		Number of times the cable modem receives an authorization reject message.
docsBpiCmAuthInvalids		Number to times the cable modem receives an authorization invalid message.
docsBpiCmAuthRejectErrorCode The options are:		Enumerated description of the error code in the most recent authorization reject message the cable modem receives.
	none	No authorization reject messages have been received since reboot.
	unknown	Last error code value was zero.
	unauthorized cm	The cable modem received an Authorization Reject in response to an Authorization Request with an error code of 1 (unauthorized cable modem).
	unauthorized SID	The cable modem received an Authorization Reject in response to an Authorization Request with an error code of 2 (unauthorized SAID).
docsBpiCmAuthRejectErrorString		The display string in the most recent authorization reject message the cable modem receives since reboot. If no authorization has been received, this value is zero.

Field Output		Description
docsBpiCmAuthInvalidErrorCode		Enumerated description of the error code in the most recent authorization invalid message that the cable modem receives.
	none	No authorization invalid messages have been received since reboot.
	unknown	Last error code value was zero.
	unauthorized cm	The cable modem received an Authorization Invalid message from the CMTS with an error code of 1 (unauthorized cable modem). This indicates that the CMTS and cable modem have lost authorization key synchronization.
	unauthorized SID	The cable modem received a Key Reject with an error code of 2 (unauthorized SAID).
docsBpiCmAuthInvalidErrorString		Display string in most recent Authorization Invalid message received by the cable modem.

Table 22-12 BPI > BPI TEK Parameters

Field Output	Description
docsBpiCmTEKPrivacyEnable	Identifies if this SID is provisioned to run Baseline Privacy.
docsBpiCmTEKState	State of the indicated TEK FSM. The options are: ■ Start ■ OPWait ■ OpReauthWait ■ Operational ■ Rekey Wait ■ Rekey Reauth Wait
docsBpiCmTEKExpiresOld	Actual clock time for expiration of the immediate predecessor of the most recent TEK for this FSM.
docsBpiCmTEKExpiresNew	Actual clock time for expiration of the most recent TEK for this FSM.
docsBpiCmTEKKeyRequests	Number of times the cable modem transmits a key request message.
docsBpiCmTEKKeyReplies	Number of times the cable modem receives a key reply message, including a message whose authentication fails.
docsBpiCmTEKKeyRejects	Number of times the cable modem receives a key reject message, including a message whose authentication fails.
docsBpiCmTEKInvalids	Number of times the cable modem receives a TEK invalid message, including a message whose authentication fails.
docsBpiCmTEKAuthPends	Number of times an authentication pending event occurs in this FSM.
docsBpiCmTEKKeyRejectErrorCode	Enumerated description of the error-code in most recent key reject message received by the cable modem.
none	No key reject message has been received since reboot.
unknown	Last error-code was zero.
unauthorized SID	SID was unauthorized.

Field Output	Description
docsBpiCmTEKKeyRejectErrorCode	Display string in the most recent key reject message received by the cable modem. This displays a zero length string if no key reject message has been received since reboot.
docsBpiCmTEKKeyRejectErrorString	Display string in most recent key reject message received by the cable modem.
docsBpiCmTEKInvalidErrorCode	Enumerated description of the error code in the modem recent TEK invalid message reviewed by the cable modem.
None	No TEK invalid message has been received since reboot.
unknown	Last error code was zero.
invalid key sequence	Invalid key sequence.
docsBpiCmTEKInvalidErrorString	Display string in the most recent TEK invalid message received by the cable modem. If no TEK invalid message has been received since reboot, this value displays as a zero length string.

Table 22-13 BPI > BPI Plus Base Parameters

Field Output	Description
docsBpi2CmPrivacyEnable	Indicates if the cable modem is provisioned to run Baseline Privacy Plus.
docsBpi2CmPublicKey	Indicates the DER-encoded RSAPublicKey ASN.1 type string, as defined in the RSA Encryption Standard (PKCS #1) [10], corresponding to the public key of the cable modem. The 74, 106, 140, 204, and 270 byte key encoding lengths correspond to 512 bit, 768 bit, 1024 bit, 1536 bit, and 2048 public moduli respectively.
docsBpi2CmAuthState The options are:	State of the cable modem authorization Finite State Machine (FSM).
Start	FSM is in its initial state.
authwait	The cable modem has received the "Provisioned" event, indicating that it has completed RF MAC registration with the CMTS. In response to receiving the event, the cable modem has sent both an Authentication Information and an Authorize Request message to the CMTS and is waiting for the reply.
Authorized	The cable modem has received an Authorization Reply message which contains a list of valid SAIDs for this cable modem. At this point, the modem has a valid Authorization Key and SAID list. Transition into this state triggers the creation of on TEK FSM for each of the cable modem's privacy-enabled SAIDs.
ReauthWait	The cable modem has an outstanding re-authorization request. The cable modem was either about to time out its current authorization or received an indication (an Authorization Invalid message from the CMTS) that its authorization was no longer valid. The cable modem sent an Authorization Request message to the CMTS and is waiting for a response.

Field Output		Description
	Auth Reject Wait	The cable modem received an Authorization Reject message in response to its last Authorization Request. The Authorization Reject's error code indicated that the error was not of a permanent nature. In response to receiving this reject message, the cable modem set a timer and transitioned to the Authorized Reject Wait state. The cable modem remains in this state until the timer expires.
	Silent	The cable modem received an Authorization Reject message in response to its last Authorization Request. The Authorization Reject's error code indicated the error was of a permanent nature. This triggers a transition to the Silent state, where the cable modem is not permitted to pass CPE traffic, but is able to respond to SNMP management requests arriving from across the cable network.
docsBpi2CmAuthKeySequence Number		Most recent authorized key sequence number of this FSM.
docsBpi2CmAuthExpiresOld		Actual clock time for expiration of the immediate predecessor of the most recent authorization key for this FSM. If this FSM has only one authorization key, then the value is the time of activation of this FSM.
docsBpi2CmAuthExpiresNew		Actual clock time for expiration of the most recent authorization key for this FSM.
docsBpi2CmAuthReset		Determines the reauthorize event status.
The options are:		
	True	Generates a reauthorize event in the authorization FSM
	False	Does not generate an authorization event.
docsBpi2CmAuthGraceTime		Grace time for an authorization key. A cable modem is expected to start trying for a new authorization key beginning the grace time number of seconds before the authorization key actually expires.

Field Output	Description
docsBpi2CmTEKGraceTime	TEK Grace Time in seconds before TEK expires.
docsBpi2CmAuthWaitTimeout	Retransmission interval, in seconds, of Authorization Request messages from the Authorize Wait state.
docsBpi2CmReauthWaitTimeout	Retransmission interval, in seconds, of Authorization Request messages from the Authorize Wait state.
docsBpi2CmOpWaitTimeout	Retransmission interval, in seconds, of Key Requests from the Operational Wait state.
docsBpi2CmRekeyWaitTimeout	Retransmission interval, in seconds, of Key Requests from the Rekey Wait state.
docsBpi2CmAuthRejectWaitTimeou	Amount of time a CM waits (seconds) in the Authorize Reject Wait state after receiving an Authorization Reject.
docsBpi2CmSAMapWaitTimeout	Retransmission interval, in seconds, of SA Map Requests from the MAP Wait state.
docsBpi2CmSAMapMaxRetries	Maximum number of Map Request retries allowed.
docsBpi2CmAuthentInfos	Number of times the CM has transmitted an Authentication Information message.
docsBpi2CmAuthRequests	Number of times the cable modem has transmitted an authorization request message.
docsBpi2CmAuthReplies	Number of times the cable modem has receive an authorization reply message.
docsBpi2CmAuthRejects	Number of times the cable modem has received an authorization reject message.
docsBpi2CmAuthInvalids	Number of times the cable modem has received an authorization invalid message.
docsBpi2CmAuthRejectErrorCode The options are:	Enumerated description of the error code in the most recent authorization reject message the cable modem receives.
none	No authorization reject messages have been received since reboot.
unknown	Last error code value was zero.

Field Output		Description
	unauthorized cm	The cable modem received an Authorization Reject in response to an Authorization Request with an error code of 1 (unauthorized cable modem).
	unauthorized SAID	The cable modem received an Authorization Reject in response to an Authorization Request with an error code of 2 (unauthorized SAID).
	permanent Authorization Failure	Permanent authorization failure, which indicates a number of different error conditions affecting the BPKM authorization exchange including: ■ Unknown manufacturer (CMTS does not have the CA certificate) belonging to the issuer of a CM certificate. ■ CM certificate has an invalid signature. ■ ASN.1 parsing failure during verification of CM certificate. ■ CM certificate is on the "hot list". ■ Inconsistencies between certificate data and data in accompanying BPKM attributes. ■ CM and CMTS have incompatible security capabilities.
	timeOfDay NotAcquired	Time of day not acquired.
docsBpi2CmAuthRejectErrorString		Display string in the most recent authorization reject message the cable modem receives since reboot. If no authorization has been received, this value is zero.
docsBpi2CmAuthInvalidErrorCode		Enumerated description of the error code in the most recent authorization invalid message that the cable modem receives.
	none	No authorization invalid messages have been received since reboot.
	unknown	Last error code value was zero.

Field Output		Description
	unauthorized cm	The cable modem received an Authorization Invalid message from the CMTS with an error code of 1 (unauthorized cable modem). This indicates that the CMTS and cable modem have lost authorization key synchronization.
	unsolicited	Unsolicited.
	invalidkey sequence	Invalid key sequence number.
	keyRequest Authentication Failure	Message (key request) authentication failure.
docsBpi2CmAuthInvalidErrorString		Display string in most recent Authorization Invalid message received by the cable modem.

Table 22-14 BPI > BPI Plus TEK Parameters

Field Output	Description
docsBpi2CmTEKSAType	Type of security association. The options are: ▪ none ▪ primary ▪ static ▪ dynamic
docsBpi2CmTEKData EncryptAlg	Data encryption algorithm being used. The options are: ▪ none ▪ des56cbcmode ▪ des40cbcmode
docsBpi2CmTEKData AuthentAlg	Data authentication algorithm being used.
docsBpi2CmTEKState	State of the indicated TEK FSM. The options are:
start	The FSM is in the initial state.
opwait	The TEK state machine has sent its initial request (Key Request) for its SAID's keying material (traffic encryption key and CBC initialization vector), and is waiting for a reply from the CMTS.
opreauthwait	This is the wait state in which the TEK state machine is placed if it does not have valid keying material while the Authorization state machine is in the middle of a reauthorization cycle.
Operational	The cable modem has valid keying material for the associated SAID.
Rekey Wait	The TEK Refresh Timer has expired and the cable modem has requested a key update for this SAID. Note that the newer of its two TEKs has not expired and can still be used for both encrypting and decrypting data traffic.
Rekey Reauth Wait	This is the wait state in which the TEK state machine is placed if the TEK state machine has valid traffic keying material, has an outstanding request for the latest keying material, and the Authorization State Machine initiates a reauthorization cycle.

Field Output	Description
docsBpi2CmTEKKey Sequence Number	Most recent TEK key sequence number for this TEK FSM.
docsBpi2CmTEKExpiresOld	Actual clock time for expiration of the immediate predecessor of the most recent TEK for this FSM.
docsBpi2CmTEKExpiresNew	Actual clock time for expiration of the most recent TEK for this FSM.
docsBpi2CmTEKKeyRequest s	Number of times the cable modem transmits a key request message.
docsBpi2CmTEKKeyReplies	Number of times the cable modem receives a key reply message, including a message whose authentication fails.
docsBpi2CmTEKKeyRejects	Number of times the cable modem receives a key reject message, including a message whose authentication fails.
docsBpi2CmTEKInvalids	Number of times the cable modem receives a TEK invalid message, including a message whose authentication fails.
docsBpi2CmTEKAuthPends	Number of times an authentication pending event occurs in this FSM.
docsBpi2CmTEKKeyReject Error Code	Enumerated description of the error-code in most recent key reject message received by the cable modem.
none	No key reject message has been received since reboot.
unknown	Last error-code was zero.
unauthorized SAID	SAID was unauthorized.
docsBpi2CmTEKKeyReject Error String	Display string in the most recent key reject message received by the cable modem. This displays a zero length string if no key reject message has been received since reboot.
docsBpi2CmTEKInvalidError Code	Enumerated description of the error code in the modem recent TEK invalid message reviewed by the cable modem.
None	No TEK invalid message has been received since reboot.
unknown	Last error code was zero.
invalid key sequence	Invalid key sequence.

Field Output	Description
docsBpi2CmTEKInvalidError String	Display string in the most recent TEK invalid message received by the cable modem. If no TEK invalid message has been received since reboot, this value displays as a zero length string.

Table 22-15 System Parameters

Field Output	Description
Descriptor	Provides a textual description of the cable modem vendor.
Contact	A contact person for the network.
Name	The name of the network device.
Location	Location of the network device.

Table 22-16 Device > Device Configuration Parameters

Field Output	Description
Serial Number	Manufacturer's serial number for this device.
STP Control	Controls operation of the spanning tree protocol (as distinFieldshed from transparent bridging). Values are:
stEnabled	Spanning tree protocol is enabled, subject to bridging constraints.
noStFilter Bpdu	Spanning tree is not active, and Bridge PDUs received are discarded.
noStPass Bpdu	Spanning tree is not active and Bridge PDUs are transparently forwarded.
SW Server	IP address of the TFTP server used for software upgrades. If the TFTP server is unknown, 0.0.0.0 is displayed.
SW Filename	Filename of the software image to be loaded into this device. Unless set via SNMP, this is the file name specified by the provisioning server that corresponds to the software version that is desired for this device. If the filename is unknown, the string “unknown” is returned.
Admin Status	Current provisioning administrative status. Values include:

Field Output	Description
Upgrade FromMgt	Device will initiate a TFTP software image download. After successfully receiving an image, the device will set its state to IgnoreProvisioningUpgrade and reboot. If the download process is interrupted by a reset or power failure, the device will load the previous image and, after re-initialization, continue to attempt loading the image.
Allow Provisioning Upgrade	Device will use the software version information supplied by the provisioning server when next rebooting (this does not cause a reboot). This status appears at initial startup.
Ignore Provisioning Upgrade	Device will disregard software image upgrade information from the provisioning server.
Oper Status	Current provisioning operational status. Values include:
InProgress	A TFTP download is underway, either as a result of a version mismatch at provisioning or as a result of an upgradeFromMgt request.
Complete From Provisioning	The last software upgrade was a result of version mismatch at provisioning.
Complete FromMgt	The last software upgrade was a result of setting docsDevSwAdminStatus to upgradeFromMgt.
Failed	The last attempted download failed, ordinarily due to TFTP timeout.
Other	State other than the ones described above.
Current Version	Software version currently operating in this device.
Boot State	Current boot state. Values include:
Operational	Device has completed loading and processing of configuration parameters and the CMTS has completed the Registration exchange.
Disabled	Device was administratively disabled, possibly by being refused network access in the configuration file.
WaitingFor DhcpOffer	A DHCP Discover has been transmitted and no offer has yet been received.
WaitingFor Dhcp Response	A DHCP Request has been transmitted and no response has yet been received.
WaitingFor TimeServer	A Time Request has been transmitted and no response has yet been received.

Field Output	Description
WaitingFor Tftp	A request to the TFTP parameter server has been made and no response has been received.
RefusedBy Cmts	The Registration Request/Response exchange with the CMTS failed.
Forwarding Denied	The registration process completed, but the network access option in the received configuration file prohibits forwarding.
Other	State other than the ones described above.
Unknown	Unknown state.
DHCP Server	IP address of the DHCP server that assigned an IP address to this device. This field displays 0.0.0.0 if DHCP was not used for IP address assignment.
Time Server	IP address of the Time server (RFC-868). This field displays 0.0.0.0 if the time server IP address is unknown.
TFTP Server	IP address of the TFTP server responsible for downloading provisioning and configuration parameters to this device. This field displays 0.0.0.0 if the TFTP server address is unknown.
Server Config File	Name of the device configuration file read from the TFTP server. This field displays an empty string if the configuration file name is unknown.

Table 22-17 Device > Event Configuration Parameters

Field Output	Description
Syslog Server	IP address of the Syslog server. If the value is 0.0.0.0, the syslog transmission is inhibited.
Threshold	Number of trap/syslog events per Throttle Interval to transmit before throttling.
Interval (seconds)	Interval over which the trap threshold applies. At initial startup, this value is one.
Admin Status The options are:	Controls the transmission of traps and syslog messages with respect to the trap pacing threshold. A single event is counted as a single event for threshold counting. That is, an event causing both a trap and a syslog message is still considered a single event.
unconstrained	Causes traps and syslog messages to transmit without regard for threshold settings. At initial startup, this is the default.
maintainBelowThreshold	Causes the suppression of trap transmission and syslog messages if the number of traps would otherwise exceed the threshold.
stopAtThreshold	Causes trap transmission to cease at the threshold, and not resume until you manually intervene.
inhibited	Causes the suppression of all trap transmission and syslog messages.
Inhibited	Indicates whether the trap and syslog transmission is inhibited because of thresholds or the current settings of the Throttle Admin parameter.

Table 22-18 Device > Events Parameters

Field Output	Description
First Time	Creation time for the entry.
Last Time	If multiple events are reported through the same entry, the time that the last event for this entry occurred.
Counts	Number of consecutive event instances reported by this entry.
Level	Priority level for this event, as defined by the vendor. These are ordered from most serious (emergency) to least serious (debug). The options are: ▪ emergency ▪ alert ▪ critical ▪ error ▪ warning ▪ notice ▪ information ▪ debug
ID	Unique identifier the type of event.
Text	Description of the event.

Table 22-19 Device > Event Control Parameters

Field Output	Description
Priority	The priority level of the particular event that occurred for the particular cable modem. Priority levels are ordered from the most serious to the least serious. The priority levels are: ■ emergency ■ alert ■ critical ■ error ■ warning ■ notice ■ information ■ debug
Action	Determines how the event notification is sent.
Local Reporting	The event logs to the internal log.
Traps Reporting	The event logs generate a trap.
Syslog Reporting	A syslog message is sent.

Table 22-20 Interfaces Parameters

Field Output	Description
Description	Identifies the interface.
Type	Type of interface.
Admin Status	Desired state of the interface. When the CMTS initalizes, all interfaces are down. You must either manually or configure the interfaces to be in a testing state or be up.
Oper Status	Current operational state of the interface.
The options are:	
up	Interface is operating normally and is ready to pass packets.
down	Interface is not operating.
testing	No operational packets can be passed.
unknown	State of the interface cannot be determined
dormant	Interface is ready to transmit and receive network traffic.
In Octets	Total number of octets the interface receives, including framing characters.
In Unicast Packets	Number of packets, delivered to this sub layer to a higher sublayer that were not addressed to a multicast or broadcast address at this sub-layer.
In Multicast Packets	Number of packets, delivered by this sub layer to a higher sub layer that were not addressed to a multicast address at this sub layer.
In Broadcast Packets	Number of packets, delivered to this sub-layer to a higher sub layer that were not addressed to a broadcast address at this sub layer.
In Errors	Number of inbound packets that contain errors preventing them from being deliverable to a higher layer protocol.
In Discards	Number of inbound packets that were chosen to be discarded even though no errors were detected to prevent their being deliverable to a higher layer protocol. The reason for discarding the packets could be to free up buffer space.
Out Octets	Number of packets received through the interface that were discarded because of an unknown or unsupported protocol.

Field Output	Description
Out Unicast Packets	Total number of packets that higher level protocols requested be transmitted and were not addressed to a multicast or broadcast address at this sub layer, including those that were discarded or not sent.
Out Multicast Packets	Total number of packets that higher level protocols request be transmitted and were addressed to a multicast address at this sub layer.
Out Broadcast Packets	Total number of packets that higher level protocols requested to be transmitted and were addressed to a broadcast address at this sub layer, including those that ere discarded or not sent.
Out Errors	Number of outbound packets that could not be transmitted because of errors.
Out Discards	Number of outbound packets that were chosen to be discarded even though no errors had been detected to prevent their being transmitted.

Table 22-21 MTA > Base Parameters

Field Output	Description
Serial Number	Manufacturer’s serial number for this MTA.
Hardware Version	Manufacturer’s hardware version for this MTA.
MAC Address	Telephony MAC address for this addrss
Fully Qualified Domain Name	Fully qualified domain name for this MTA.
End Points	Physical end points for this MTA.
Voice Enabled	MTA admininistrive status for this device. The options are: ■ True: Voice is enabled ■ False: Voice is disabled
Type ID	Device type identifier for the DHCP option 60 exchanged between the MA and the DHCP server.
Provisioned State	Indicates the completion state of the provisioning process. The options are: ■ Pass: Pass state occurs after completing the processing of the configuration file. ■ In Progress: Occurs from boot time until configuration file processing is complete. ■ Fail: Pass state occurs after completing the processing of the configuration file. Manual intervention is required.
HTTP Access	Indicates whether HTTP file access is supported for MTA configuration file transfer.

Table 22-22 MTA > Server Parameters

Field Output	Description
Boot State	The state of the server. The options are: ■ Operational: Device is done loading and processing configuration parameters, and the CMTS has completed the registration exchange. ■ Disabled: Device was administratively disabled, possibly by being refused network access in the configuration file. ■ waiting for Dhcp Offer: DHCP discover has been transmitted and no offer has been received. ■ Waiting for Dhcp Response: DHCP request has been trasmitted and no response has yet been received. ■ Waiting For Config: Request for configuration server has been made and no response received. ■ Refused by CMTS: Registration request/response exchanged with the CMTS failed. ■ Other: Other reason besides those listed above. ■ Unknown: The state is unknown.
DHCP Server	IP address or fully qualified domain name (FQDN) of the DHCP server that assigned an address to this device. This value is 0.0.0.0 if the DHCP derver is not used for the IP assignment address.
Primary DNS Server	IP address for FQDN of the primary DNS server that resolved an IP address for this device.
Secondary DNS Server	IP address or FQDN of the secondary DNS server that resolved an IP address for this device.
Configuration File	URL of the TFTP/HTTP file for downloading provisioning and configuration parameters to this device. This is a value of null is the server address is unknown.
SNMP Entity	IP address or FQDN of the SNMP entity for provisioning trap handling that assigned an IP address to this device. This value is 0.0.0.0 if DHCP was not used for IP address assignment.

Table 22-23 MTA > NCS > End Points Parameters

Field Output	Description
Call Agent ID	The call agent name. The call agent name can be a FQDN or an IP address.
Call Agent UDP Port	The call agent UDP port for this instance of call signalling.

Table 22-24 MTA > NCS > Codec Parameters

Field Output	Description
Index	Index for this codec.
Type	CODEC conversion types that are supported by the MTA: ■ g729 ■ g729a ■ g729e ■ g711mu ■ g726 ■ g728

Table 22-25 MTA > NCS > Configuration Parameters

Field Output	Description
Echo Cancellation	Displays whether echoes are cancelled (True or False). True indicates that echo cancellation is in use. False indicates that echo cancellation is not in use.
Silence Suppression	Displays whether silence is suppressed in the send direction (True or False). True indicates that silence suppression is enabled. False indicates that silence suppression is disabled.
Connection Mode	Displays the various ways in which the MTA can connect to the network (such as voice, fax, and modem).
R0 Cadence	Displays ring cadence intervals, where each bit represents a duration of 200 milliseconds (6 second total).
R6 Cadence	Displays ring cadence intervals, where each bit represents a duration of 200 milliseconds (6 second total).
R7 Cadence	Displays ring cadence intervals, where each bit represents a duration of 200 milliseconds (6 second total).
Def Call Signal TOS	Displays the default Type of Service (TOS) value for call signalling (signals for setting up calls) in the IP header.
Def Media Stream TOS	Displays the default Type of Service (TOS) value for media stream packets in the IP header. Audio and video streams are examples of media streams.

Field Output	**Description**
TOS Format Selector	Displays one of the following formats for the default call signalling and media stream TOS values: ■ dscpCodepoint – Specifies that the TOS field is treated as a Differentiated Service Code Point (DSCP). The TOS field in the IP header identifies the differentiated service per hop behavior, which enables intermediate routers to select packets and apply specific forwarding rules based on the value of the TOS byte. ■ ipv4TOSOctet – Specifies that the TOS field is treated as an IPv4 TOS octet. Networks can provide a specific level of service based on the octet value in the packet.

A CONFIGURING EXTERNAL PROVISIONING SERVERS

A DHCP server is required for cable modems, MTAs, and CPE devices to boot and receive their IP configuration information — such as IP address and host options.

DHCP servers fall into two categories:

- **External** — DHCP servers that reside on systems other than your local Cuda 12000 (that is, the Cuda 12000 that has the cable interface that you are configuring). DHCP messages are forwarded over the network to a remote, external DHCP server. The external DHCP server can be a FastFlow Broadband Provisioning Manager (FastFlow BPM) DHCP server running on another system or a third-party provisioning server running on another system.
- **Internal** — A FastFlow BPM DHCP server that resides on the same Cuda 12000 that has the cable interface you are configuring (that is, the local Cuda 12000). DHCP requests are forwarded internally to the FastFlow DHCP server. The FastFlow BPM is an optional product that may or may not be installed on your Cuda 12000.

If you are not using the internal FastFlow BPM DHCP server and are instead using an external DHCP server, then you *must* point the DHCP relay agent on the CMTS DOCSIS/EuroDOCSIS module to the IP address of the external provisioning server. The following procedure steps you through the process of configuring the CMTS to use an external DHCP provisioning server.

Configuring the DHCP Server

The purpose of DHCP Server configuration is to add a DHCP Server, to which DHCP Relay requests are forwarded. DHCP Servers are assigned on a per interface basis.

If a DHCP server is not configured, then the DHCP relay drops all DHCP requests as it does not know where to forward them.

Adding DHCP Servers

⚠ ***NOTE:*** *You must have access privileges to the Provisioning functional area to be able to add DHCP Servers. For more information about access privileges, refer to chapter “Managing User Accounts”on page page 93.*

From **Network Browser,** navigate to **Cuda Chassis Manager>Configuration>IP>DHCP Relay.** To add a DHCP Server follow these steps:

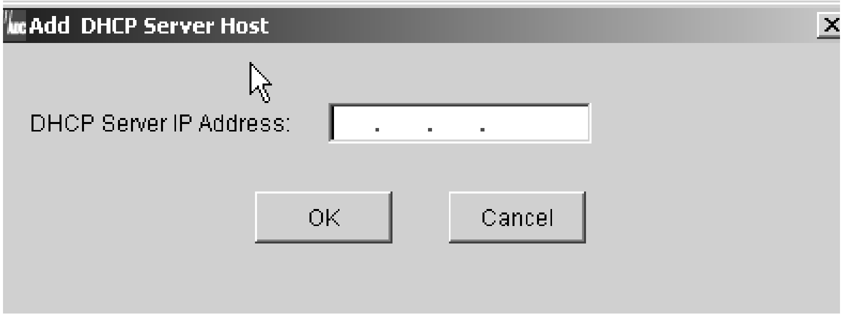
1. From the Summary window, select the row that includes the interface to which you want to add the DHCP Server, for the external provisioning server.

2 Choose the **DHCP Relay**.

3. Go to the **Servers** tab, which displays DHCP Servers already assigned to that interface. For example, if the display is empty it means that there are no DHCP Servers assigned to that interface.

4. Choose **Add** to open the **Add DHCP Server Host** box.

Figure A - 1 Add DHCP Server Host Box Display



5. Enter the DHCP Server IP address to be used for the external provisioning server, on the selected interface.

6. Click **OK** to save the setting; or click **Cancel** to exit “Add DHCP Server Host,” without saving the configuration.

B GLOSSARY

16 QAM

Modulation mode used by the CMTS. QAM uses both amplitude and phase modulation to encode multiple bits of data in one signaling element, thus achieving higher data transfer rates than just amplitude or phase modulation alone.

16 QAM encodes four bits per symbol as one of sixteen possible amplitude and phase combinations. 16 QAM refers to the number of discrete phase/amplitude states that are used to represent data bits.

64 QAM

A modulation mode used by the CMTS. 64 QAM uses both amplitude and phase modulation to encode multiple bits of data in one signaling element. 64 QAM encodes 6 bits per symbol as one of 64 possible amplitude and phase combinations.

256 QAM

A modulation mode used by the CMTS. 256 QAM uses both amplitude and phase modulation to encode multiple bits of data in one signaling element. 64 QAM encodes 8 bits per symbol as one of 256 possible amplitude and phase combinations.

A

Record that contains the IP address of the record’s owner. Since hosts may have multiple IP addresses, multiple A records may match a given domain name.

Address Resolution Protocol (ARP)

A protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network. For example, in IP Version 4, the most common level of IP in use today, an address is 32 bits long. In an Ethernet local area network, however, addresses for attached devices are 48 bits long. (The physical machine address is also known as a Media Access Control or MAC address address.)

American National Standards Institute (ANSI) The primary organization for fostering the development of technology standards in the United States.

ARP See Address Resolution Protocol.

Bandwidth Allocation Map The downstream MAC Management Message that the CMTS uses to allocate transmission opportunities to CMs.

Baseline Privacy Interface Provides data privacy for DOCSIS 1.0 CMs and CMTS. BPI+, provides privacy for DOCSIS 1.1 CMs and CMTS.

BDU See Bridge Protocol Data Unit.

Bootstrap Protocol (BOOTP) A protocol that lets a network user be automatically configured (receive an IP address) and have an operating system boot or initiated without user involvement. The BOOTP server, managed by a network administrator, automatically assigns the IP address from a pool of addresses for a certain duration of time.

BPI See Baseline Privacy Interface.

Bridge Protocol Data Unit (BDU) Spanning tree protocol messages as defined in [ISO/IEC10038].

Broadband Network technology that multiplexes multiple, independent network carriers onto a single cable or fiber. The technology is used to carry voice, video, and data over the same cable or fiber.

Broadcast Transmission to two or more devices at the same time, such as over a bus-type local network or by satellite; protocol mechanism that supports group and universal addressing.

Broadcast Addresses A predefined destination address that denotes the set of all data network service access points.

Cable Modem (CM) A modulator-demodulator at subscriber locations intended for use in conveying data communications on a cable television system.

Cable Modem Termination System (CMTS) A device located at the cable system head-end or distribution hub, that interfaces the HFC network to local or remote IP networks.

Cable Modem Termination System - Network Side Interface (CMTS-NSI)
The interface, defined in [DOCSIS3], between a CMTS and the equipment on its network side.

Cable Modem to CPE Interface (CMCI)
The interface, defined in [DOCSIS4], between a CM and CPE.

Carrier Hum Modulation
The peak-to-peak magnitude of the amplitude distortion relative to the RF carrier signal level due to the fundamental and low-order harmonics of the power-supply frequency.

Carrier-to-Noise Ratio (C/N or CNR)
The voltage difference between the digitally-modulated RF carrier and the continuous random noise. CNR is measured in decibels (dB).

CM
See Cable Modem.

CMCI
See Cable Modem to CPE Interface.

CMTS
See Cable Modem Termination System.

C/N or CNR
See Carrier-to-Noise Ratio.

CNAME
A record that contains an alias or nickname for the official domain name (also known as the canonical name).

Cross-Modulation
A form of television signal distortion where modulation from one or more television channels is imposed on another channel or channels.

Customer Premises Equipment (CPE)
Equipment at the end user’s premises. This equipment may be provided by the end user or the service provider.

Data Link Layer
Layer 2 in the Open System Interconnection (OSI) architecture; the layer that provides services to transfer data over the transmission link between open systems.

DHCP
See Dynamic Host Configuration Protocol.

Distribution Hub
A location in a cable television network which performs the functions of a head-end for customers in its immediate area, and which receives some or all

of its television program material from a Master Head-end in the same metropolitan or regional area.

DNS See Domain Name System.

DOCSIS Data Over Cable Service Interface Specification, developed by CableLabs. Defines interface standards for cable modems transmission and supporting equipment.

Domain Name System (DNS) An on-line, distributed database used to map human-readable machine names into IP address for resolving machine names to IP addresses.

Downstream The direction of data flow from the head-end (CMTS) to the subscriber (CM).

Drop Cable Coaxial cable that connects to a residence or service location from a directional coupler (tap) on the nearest coaxial feeder cable.

Dynamic Host Configuration Protocol (DHCP) A protocol that allows dynamic assignment of IP addresses to CPEs. DHCP is also used to assign IP addresses to CMs.

Dynamic Range The ratio between the greatest signal power that can be transmitted over a multichannel analog transmission system without exceeding distortion or other performance limits, and the least signal power that can be utilized without exceeding noise, error rate or other performance limits.

Ethernet A networking standard running speeds of 1 Gbps (Gigabit Ethernet), 10 Mbps (10BaseT) or 100 Mbps (100BaseT). Ethernet typically uses twisted pair wiring or optical fiber.

EuroDOCSIS European Data Over Cable Service Interface Specification, developed by tComLabs and CableLabs. Defines interface standards for cable modems transmission and supporting equipment.

Extended Subsplit A frequency division scheme that allows bidirectional traffic on a single coaxial cable. In the U.S., reverse path signals come to the head-end from 5 to 42 MHz. Forward path signals go from the head-end from 50 or 54 MHz to the upper frequency limit.

FDDI See Fiber Distributed Data Interface.

FEC See Forward Error Correction.

Feeder Cable Coaxial cables that run along streets within the served area and connect between the individual taps which serve the customer drops.

Fiber Node The interface between a fiber trunk and the coaxial distribution. Fiber nodes are located in a subscribers neighborhood.

File Transfer Protocol (FTP) A protocol that allows users to log into a remote system, identify themselves, list remote directories, and copy files to and from the remote machine. FTP understands a few basic file formats. It is more complex than Telnet in that it maintains separate TCP connections for control and data transfer.

Flow A unidirectional data path between a cable modem and a CMTS.

Forward Error Correction (FEC) A technique for correcting errors incurred in transmission over a communications channel by the receiver, without requiring the retransmission of any information by the transmitter; typically it involves a convolution of the transmitted bits and the appending of extra bits, using a common algorithm by both the receiver and transmitter.

FTP See File Transfer Protocol.

Gateway A device that communicates with two protocols and translates services between them.

Graphical User Interface (GUI) A program that displays information using graphics instead of command line text. The user can interact with a computer operating system through a series of "windows", also known as "point and click"

Group Delay The difference in transmission time between the highest and lowest of several frequencies through a device, circuit or system.

Guard Time Minimum time allocated between bursts in the upstream referenced from the symbol center of the last symbol of a burst to the symbol center of the first symbol of the following burst. The guard time should be at least the duration of five symbols plus the maximum system timing error.

GUI See Graphical User Interface.

Harmonic Related Carrier (HRC) A method of spacing television channels on a cable television system in exact 6-MHz increments, with all carrier frequencies harmonically related to a common reference.

Head-End The central location on the cable network that originates the broadcast video and other signals in the downstream direction. See also Master Head-end, Distribution Hub.

Header Protocol control information located at the beginning of a protocol data unit.

HF See High Frequency.

HFC See Hybrid Fiber/Coaxial.

High Frequency (HF) The entire subsplit (5-30 MHz) and extended subsplit (5-42 MHz) band used in reverse channel communications over the cable television network.

High Return A frequency division scheme that allows bi-directional traffic on a single coaxial cable. Reverse channel signals propagate to the head-end above the downstream passband.

HRC See Harmonic Related Carrier.

Hum Modulation Undesired modulation of the television visual carrier by the fundamental or low-order harmonics of the power supply frequency, or other low-frequency disturbances.

Hybrid Fiber/Coaxial (HFC) System A broadband bidirectional shared-media transmission system using fiber trunks between the head-end and the fiber nodes, and coaxial distribution from the fiber nodes to the customer locations.

Hybrid Fiber/Coaxial (HFC) Network A network where the trunk of the cable plant is fiber technology. The fiber is connected to a coaxial cable and the signal is converted so that it is compatible to that media. The coaxial cable runs through the branches of the network and is dropped into the subscriber’s home.

ICMP See Internet Control Message Protocol.

IEEE See Institute of Electrical and Electronic Engineers.

IETF See Internet Engineering Task Force.

IGMP See Internet Group Management Protocol.

Impulse Noise Noise characterized by non-overlapping transient disturbances.

Incremental Related Carriers (IRC) A method of spacing NTSC television channels on a cable television system in which all channels except 5 and 6 correspond to the standard channel plan, used to reduce composite triple beat distortions.

Information Element The fields that make up a MAP and define individual grants, deferred grants, etc.

Ingress Noise A type of noise that is the major source of cable system noise. It is caused by discrete frequencies picked up by the cable plant from marine and radio broadcasts or from improperly grounded or shielded home appliances such as a hair dryer.

Initial Ranging A process in which a cable modem acquires the correct timing offset so that it can accurately transmit using the correct mini-slot. Each cable modem obtains a timing offset; the timing offset depends on the time difference of the distance of the cable modem from the CMTS. Initial ranging is performed at cable modem initialization.

Institute of Electrical and Electronic Engineers (IEEE) An organization of electrical engineers. The IEEE fosters the development of standards that often become national and international standards. Many IEEE standards are network interface standards.

International Organization for Standardization (ISO) An international standards body, commonly known as the International Standards Organization.

International Telecommunications Union (ITU-T) The Telecommunication Standardization Sector of the International Telecommunications Union is the primary international body for fostering cooperative standards for telecommunications equipment and systems.

Internet Control Message Protocol (ICMP) An Internet network-layer protocol.

Internet Engineering Task Force (IETF) A group that defines standard Internet operating protocol, such as TCP/IP.

Internet Group Management Protocol (IGMP)
A network-layer protocol for managing multicast groups on the Internet. IGMP establishes and maintains a database of group multicast addresses and the interfaces to which a multicast router must forward the multicast data packets.

Internet Protocol (IP)
The method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet. An IP address includes a network address and a host address. An IP address can also be divided by using classless addressing or subnetting.

Interval Usage Code
A field in MAPs and UCDs to link burst profiles to grants.

IP
See Internet Protocol.

IP Filtering
IP filtering enables you to filter upstream packets that pass through the CMTS. IP filtering can prevent subscribers from accessing head-end servers, enforce subscribers to log on to the cable network, enforce separately-billed service packages for data, and provide group access control for IP Multicast.

IP Multicast
IP Multicast reduces traffic on a network by delivering a single stream of information to multiple users at one time.

IP Network
A group of IP routers that route IP datagrams. These routers are sometimes referred to as Internet gateways. Users access the IP network from a host. Each network in the Internet includes some combination of hosts and IP routers.

IRC
See Incremental Related Carriers.

ISO
See International Organization for Standardization.

ITU-T
See International Telecommunications Union.

Java
A high level programming language developed by Sun Microsystems.

LAN
See Local Area Network.

Latency
The time delay, expressed in quantity of symbols, taken for a signal element to pass through a device.

Layer

A subdivision of the Open System Interconnection (OSI) architecture, constituted by subsystems of the same rank.

LDAP

See Lightweight Directory Access Protocol.

Lightweight Directory Access Protocol (LDAP)

A set of protocols for accessing information directories. LDAP is based on the standards contained within the X.500 standard, but is significantly simpler. And unlike X.500, LDAP supports TCP/IP, which is necessary for any type of Internet access to a directory server.

LLC

See Logical Link Control Procedure.

Local Area Network (LAN)

A non-public data network in which serial transmission is used for direct data communication among data stations located on the user's premises.

Logical Link Control (LLC) Procedure

In a local area network (LAN) or a Metropolitan Area Network (MAN), that part of the protocol that governs the assembling of data link layer frames and their exchange between data stations, independent of how the transmission medium is shared.

MAC

See Media Access Control.

Management Information Base (MIB)

A logical structure, used by the SNMP manager and agent, of the parameters needed for configuring, monitoring, or testing an SNMP device. The MIB is a hierarchical-naming structure used to uniquely identify SNMP objects (parameters). It is typically illustrated as an inverted tree.

Master Head-End

A head-end that collects television program material from various sources by satellite, microwave, fiber, and other means and distributes this material to Distribution Hubs in the same metropolitan or regional area. A Master Head-end MAY also perform the functions of a Distribution Hub for customers in its own immediate area.

Media Access Control (MAC) Address

A MAC address is used by the link layer protocol to forward packets “one hop at a time” between the host and the first router and between the first router and the next router and so on through the network until the packet arrives at it’s final destination.

Media Access Control (MAC) Procedure

In a subnetwork, that part of the protocol that governs access to the transmission medium independent of the physical characteristics of the medium, but taking into account the topological aspects of the subnetworks, in order to enable the exchange of data between nodes. MAC procedures include framing, error protection, and acquiring the right to use the underlying transmission medium.

Media Access Control (MAC) Sublayer The part of the data link layer that supports topology-dependent functions and uses the services of the Physical Layer to provide services to the logical link control (LLC) sublayer.

MIB See Management Information Base.

Micro-reflections Echoes in the forward transmission path due to departures from ideal amplitude and phase characteristics.

Mid Split A frequency division scheme that allows bi-directional traffic on a single coaxial cable. Reverse channel signals propagate to the head-end from 5 to 108 MHz. Forward path signals go from the head-end from 162 MHz to the upper frequency limit. The diplex crossover band is located from 108 to 162 MHz.

Mini-Slot A power-of-two multiple of 6.25 microsecond increments. For example, 1, 2, 4, 8, 16, 21, 64 or 128 times 6.25 microseconds. Mini-slots are used to divide the upstream bandwidth into discrete increments.

Moving Picture Experts Group (MPEG) A group which develops standards for digital compressed moving pictures and associated audio.

MPEG See Moving Picture Experts Group.

MSO Multi System Operator

Multimedia Terminal Adapter (MTA) A hardware interface between a computer and an Integrated Services Digital Network line needed for Voice Over IP.

Multipoint Access User access in which more than one terminal equipment is supported by a single network termination.

Multipoint Connection A connection among more than two data network terminations.

National Cable Television Association (NCTA) A voluntary association of cable television operators which, among other things, provides guidance on measurements and objectives for cable television systems in the United States.

National Television Systems Committee (NTSC) A committee which developed a set of standard protocol for television broadcast transmission and reception in the United States.

NCTA See National Cable Television Association.

NEBS See Network Equipment Building Systems.

Network Equipment Building Systems (NEBS) NEBS is a Telcordia standard defining the physical, electrical, and environmental conditions under which network equipment must operate. NEBS includes: temperature, humidity, airborne contamination, fire resistance, earthquake and vibration, noise, electrical safety, lightning and surge immunity, ESD immunity, and electro-magnetic compatibility.

Network Layer Layer 3 in the Open System Interconnection (OSI) architecture; the layer that establishes a path between open systems.

NS Record that contains the domain name of the authoritative name server for the domain.

NTSC See National Television Systems Committee.

Open Systems Interconnection (OSI) A framework of ISO standards for communication between different systems made by different vendors, in which the communications process is organized into seven different categories that are placed in a layered sequence based on their relationship to the user. Each layer uses the layer immediately below it and provides a service to the layer above. Layers 7 through 4 deal with end-to-end communication between the message source and destination, and layers 3 through 1 deal with network functions.

Open Shortest Path First (OSPF) An Interior Gateway Routing Protocol that use link-state algorithms to send routing information to all nodes in an OSPF area by calculating the shortest path to each node based on a map of the network constructed by each node. Each router sends that portion of the routing table (keeps track of routes to particular network destinations) that describes the state of its own links, and it also sends the complete routing structure of the network.

OSI See Open Systems Interconnection.

OSPF See Open Shortest Path First.

Packet Identifier (PID) A unique integer value used to identify elementary streams of a program in a single- or multi-program MPEG-2 stream.

PHY See Physical Layer.

Physical (PHY) Layer Layer 1 in the Open System Interconnection (OSI) architecture. It provides services to transmit bits or groups of bits over a transmission link between open systems and which entails electrical, mechanical, and handshaking procedures.

Physical Media Dependent (PMD) Sublayer A sublayer of the Physical Layer that transmits bits or groups of bits over particular types of transmission link between open systems. It entails electrical, mechanical, and handshaking procedures.

PID See Packet Identifier.

PMD See Physical Media Dependent Sublayer.

Protocol A set of rules and formats that determines the communication behavior of layer entities in the performance of the layer functions. It may still require an authorization exchange with a policy module or external policy server prior to admission.

PTR A record that contains a pointer to another part of the domain name space. This record is typically used in reverse zones.

QAM See Quadrature Amplitude Modulation.

QoS See Quality of Service.

Quadrature Amplitude Modulation (QAM) A method of modulating digital signals onto a radio-frequency carrier signal involving both amplitude and phase coding. This achieves a higher data transfer rate than just amplitude or phase modulation alone.

Quality of Service A networking term that specifies a guaranteed throughput level and end to end latency for traffic on the network.

Radio Frequency (RF) Signals that are used by the CMTS transmitter and receiver to send data over HFC network. A radio frequency carrier is modulated to encode the digital data stream for transmission across the cable network.

Request For Comments (RFC) A technical policy document of the IETF; these documents can be accessed on the World Wide Web at http://ds.internic.net/ds/rfcindex.html.

Return Loss The parameter describing the attenuation of a guided wave signal (e.g., via a coaxial cable) returned to a source by a device or medium resulting from reflections of the signal generated by the source.

RF See Radio Frequency.

RF DVT Radio Frequency Design Verification Test.

RFC See Request For Comments.

RIP Routing Information Protocol.

Routing Information Protocol (RIP) A routing protocol used for IP networks. The RIP protocol calculates the shortest distance between the source and destination address based on the lowest hop count.

Service Identifier (SID) A mapping between the CM and the CMTS based on which bandwidth is allocated to the CM by the CMTS and by which COS is implemented. Within a MAC domain, all SIDs are unique.

SID See Service Identifier.

Simple Network Management Protocol (SNMP) A network management protocol used to monitor IP routers, other network devices, and the networks to which they attach.

SNAP See Subnetwork Access Protocol.

SNMP See Simple Network Management Protocol.

SOA Start of Authority record. The purpose of the soa record is to inform other DNS servers how to treat information that the local server provides about the domain.

SOHO Small Office Home Office

SSRAM Synchronous Static RAM.

Subnet A network subdivided into networks or subnets. When subnetting is used, the host portion of the IP address is divided into a subnet number and a host number. Hosts and routers identify the bits used for the network and subnet number through the use of a subnet mask.

Subnet Mask A bit mask that is logically ANDed with the destination IP address of an IP packet to determine the network address. A router routes packets using the network address.

Subnetwork Access Protocol (SNAP) An extension of the LLC header to accommodate the use of 802-type networks as IP networks.

Subscriber A user in the home who accesses a data service.

Subsplit A frequency-division scheme that allows bi-directional traffic on a single cable. Reverse path signals come to the head-end from 5 to 30 (up to 42 on Extended Subsplit systems) MHz. Forward path signals go from the head-end from 50 or 54 MHz to the upper frequency limit of the cable network.

TCP See Transmission Control Protocol.

TFTP See Trivial File-Transfer Protocol.

Tick 6.25-microsecond time intervals that are the reference for upstream mini-slot definition and upstream transmission times.

Tilt Maximum difference in transmission gain of a cable television system over a given bandwidth (typically the entire forward operating frequency range).instant at which the last bit of the same PDU crosses a second designated boundary.

TLV See Type/Length/Value.

Transmission Control Protocol (TCP) A reliable stream service which operates at the transport-layer Internet protocol which ensures successful end-to-end delivery of data packets without error.

Transmission Convergence Sublayer A sublayer of the Physical Layer that provides an interface between the Data Link Layer and the PMD Sublayer.

Transmission Medium The material on which information signals may be carried; e.g., optical fiber, coaxial cable, and twisted-wirepairs.

Transport Stream In MPEG-2, a packet-based method of multiplexing one or more digital video and audio streams having one or more independent time bases into a single stream.

Trivial File-Transfer Protocol (TFTP) An Internet protocol for transferring files without the requirement for user names and passwords that is typically used for automatic downloads of data and software.

Trunk Cable Cables that carry the signal from the head-end to groups of subscribers. The cables can be either coaxial or fiber depending on the design of the system.

Type/Length/Value (TLV) An encoding of three fields, in which the first field indicates the type of element, the second the length of the element, and the third field the value.

UCD See Upstream Channel Descriptor.

UDP See User Datagram Protocol.

UHF See, Ultra-High Frequency.

Ultra-High Frequency The range of the radio spectrum is the band extending from 300 MHz to 3 GHz. The wavelengths corresponding to these limit frequencies are 1 meter and 10 centimeters.

Upstream The direction of the data flow from the subscriber location (CM) toward the head-end (CMTS).

Upstream Channel Descriptor (UCD) A MAC management message transmitted by the CMTS Adapter Module at a configured period of time. A UCD defines the characteristics of an upstream channel including the size of the mini-slot, the upstream channel ID, and the downstream channel ID. It also defines channel parameters and a burst descriptor. UCDs are transmitted for each upstream channel.

User Datagram Protocol (UDP) In conjunction with IP, UDP provides unreliable connection-less datagram delivery service. UDP can address specific protocol ports as a destination within a given host.

Very High Frequency (VHF) The range of the radio spectrum is the band extending from 30 MHz to 300 MHz. The wavelengths corresponding to these limit frequencies are 10 meters and 1 meter.

VGA Video Graphics Array display system.

VHF See Very High Frequency.

INDEX